I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Privacy Policy and Contextual Harm

MARK MACCARTHY *

CONTENTS

*Adjunct Professor, Communication, Culture and Technology Program, Georgetown University, and Senior Vice President for Public Policy, Software & Information Industry Association (SIIA). The views expressed in this article are those of the author and not necessarily those of SIIA or any of its member companies. I am grateful for comments and suggestions from attendees at the presentation of an earlier version of this paper at the June 2016 Privacy Law Scholars Conference in Washington DC.

Why, then, is the social value of privacy so isolated from the policy debate around data protection? [1]

I. INTRODUCTION

Social conceptions of privacy are a family of theories united by similar definitions of privacy, common estimations of its value and similar guidelines for policy. These three elements of definition, evaluation and policy prescription are also present in the more familiar conceptions of privacy as an individual right and as protection against harm. But in a social conception of privacy the collective, communal, group nature of privacy is primary in all three elements.

A social theory of privacy sounds like an oxymoron. Isn't privacy essentially about keeping other people out? At a very abstract level, privacy does exclude people; it does stop the flow of information to others. But a key element of a social conception of privacy is the notion that privacy does not stop the flow of information to everyone. Instead, privacy enables the flow of information to some, but not to others. A further key element of the social conceptions of privacy is the idea that the people to whom the information is allowed to flow

[1] Valerie Steeves, *Reclaiming the Social Value of Privacy*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 199 (Ian R. Kerr, Valerie M. Steeves & Carole Lucock eds., 2009).

are determined by their social role.[2] This is a critical way in which a social theory of privacy differs from the familiar individual right to control information flows, which leaves information disclosure up to the preferences of individuals. In a social theory of privacy, information flows are governed by widespread social norms.

In a social theory of privacy, the value of privacy also has an essential social dimension. In other frameworks, privacy benefits individuals – it vindicates rights that they have as human beings regardless of social structure or it protects people against certain economic harms. But in a social conception, privacy functions as an element of social structure; it maintains certain widely accepted and beneficial social practices and institutions such as law, medicine, education, democratic political governance, and religion. In this way, privacy's value is intrinsically tied to the importance and urgency of these social practices.

Finally, a social theory of privacy should contain elements of policy guidance. Here, however, social theories have been less successful. Privacy as a human right draws on the well-developed rhetoric and style of argumentation of the international human rights movement. It plausibly contrasts the fundamental nature of privacy as upholding the dignity and autonomy of individuals with the merely economic or utilitarian considerations that might justify use of private information. Privacy as harm prevention plausibly draws on the utilitarian tradition of assessing the costs and benefits of privacy protections versus their economic costs.

A social theory of privacy cannot draw on these familiar policy frameworks. For that reason, until recently it has been largely neglected in policy circles. In the last few years, however, the Federal Trade Commission,[3] the Obama Administration,[4] the new EU General

---

[2] *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 174 (2007).

[3] The Federal Trade Commission's March 2012 report recommends that for practices inconsistent with the context of their interaction with consumers, companies should give consumers choice, but that companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 36, 48 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/99JE-FBXF].

[4] The Obama Administration's consumer privacy report recommended a consumer privacy bill of rights containing a principle calling for "Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are

Data Protection Regulation,[5] and the Federal Communications Commission's proposed privacy rules for broadband providers[6] all have a key role for consistency with context. As Nissenbaum has remarked, however, this effort crucially distorts and reduces the social element in her theory, by reinterpreting the key social category of "context" as either "technology" or "business sector."[7]

One purpose of this paper is to show that a social conception of privacy can generate actionable policy guidelines. It does this by constructing a notion of harm to social contexts, and by showing how some privacy rules prevent harm to social contexts. The policy recommendation is that policymakers should assess the extent to which an information practice harms social contexts in determining whether and how to regulate.

---

consistent with the context in which consumers provide the data." WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 15 (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf [https://perma.cc/MS4K-DBQV].

[5] The new General Data Protection Regulation for the European Union calls for "consideration of context in which personal data have been collected" in determining whether further use of information is compatible with the purpose for which the data were originally collected. General Data Protection Regulation, 2016 O.J. (L 119) 37, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [https://perma.cc/ENB6-HFWK].

[6] The Federal Communications Commission's proposal for broadband privacy calls for opt-out consent for marketing communications-related services, but opt-in consent for other uses because they think that this approach is "consistent with consumer expectations" and observes the regulatory best practice that "consumer choice turns on the extent to which the practice is consistent with the context of the transaction." Notice of Proposed Rulemaking, 31 FCC Rcd. 2,500, 2,543 (2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0401/FCC-16-39A1.pdf [https://perma.cc/MKJ5-JM4P]. The FCC's final broadband privacy rule called for opt-in consent for "sensitive information" because this framework "better reflects consumer expectations." *See* In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274 (Dec. 2, 2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf [https://perma.cc/JJ7N-VAG2]. In March 2017, Congress repealed the broadband privacy rules indicating a change of direction under the new Trump Administration. *See* Cecilia Kang, *Congress Moves to Overturn Obama-Era Online Privacy Rules*, N.Y. TIMES (Mar. 28, 2017), https://www.nytimes.com/2017/03/28/technology/congress-votes-to-overturn-obama-era-online-privacy-rules.html [https://perma.cc/GEZ4-7W98].

[7] Helen Nissenbaum, *Respect for Context as a Benchmark for Privacy Online: What it is and What it isn't*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 278 (Beate Roessler & Dorota Mokrosinska eds., 2015).

Harm to a social context occurs when people withdraw from the context in order to protect themselves. This can take place, for instance, when people do not go to a doctor, lawyer, or priest or do not disclose information fully in order to avoid having the information divulged in other contexts and used against them. Of course, the harm from this less than full engagement with a social practice affects individual people, because people do not get the care and counseling they need. But that is not what I want to focus on. Isolated examples of avoidance of service practitioners suggest an idiosyncratic individual issue, not a social problem. But when avoidance is rational and widespread, the damage is social. When people generally—and with good reason—avoid doctors, lawyers, and priests, the practices of medical care, legal counseling, and religious worship do not perform the social role we expect of them.

So, harm to a social context is tied to the rational self-protective behavior of individuals to insulate themselves from adverse consequences of information uses in other contexts. This notion of harm to contexts allows a style of argumentation that justifies a substantial restriction on information flows, not on the basis of individual harm or the assertion of fundamental human rights, but on the harm that is done to a social practice. Contextual harm provides a social basis for certain restrictions on the secondary use of information.[8]

This style of argumentation goes back at least to Bentham who favored the confidentiality of the Catholic confession. He argued that when information disclosed in confession is allowed to be disclosed in court proceedings, it has the "natural effect . . . of preventing the practice"[9] of penance. It operates as a "prohibition on all such confessions for the spiritual purpose . . ."[10]

When contexts are harmed, the harm is not purely personal. The loss is not just financial, physical or psychological harm to specific

---

[8] Scholars and policymakers have attempted to distinguish permissible from impermissible secondary uses in terms of preventing harms to individuals, protecting their fundamental rights to control over information use, and respecting their reasonable expectations of how information collected by a data controller will be used. I suggest that an additional consideration is that a secondary use could be considered impermissible when it creates harm to the context in which the information was collected.

[9] 4 JEREMY BENTHAM, RATIONALE OF JUDICIAL EVIDENCE 586, 588 (Hunt & Clarke eds., 1827).

[10] *Id.* at 586.

people. Instead, the cost is social. In the example of the loss of confessional confidentiality, a certain religious practice ceases to exist as certainly as if it had been declared illegal.

In Part II of this paper, I review some of the accounts of privacy that treat it as an aspect of social structure. In particular, I look at the views of Nissenbaum, Merton, Foucault, Bloustein, Post, Regan, Steeves, and Benkler as illustrative examples of this family of privacy theories.

In Part III, I examine the contextual harm basis for several witness privileges: priest-penitent, attorney-client, psychotherapist-patient, reporter-source, and doctor-patient.

In Part IV, I discuss the notion of contextual harm and apply it to genetic privacy, student privacy, and to privacy in online social networks, thereby illustrating the utility of the notion of contextual harm in addressing some pressing privacy issues.

In Part V, I formulate a principle of contextual harm that a privacy restriction should be considered whenever an information flow causes or is likely to cause significant contextual harm. I contrast this principle with familiar privacy principles such as purpose specification and respect for context. I also seek to understand how to resolve cross-contextual conflicts where gains in one context mean losses in others, an ever-more urgent task in light of big data's capacity to aggregate and decontextualize information. Part VI is a short conclusion and summary.

While the principle of contextual harm is useful in providing a basis for many privacy restrictions, it is not complete. An information flow that causes no contextual harm might still be objectionable. Other normative bases for privacy restrictions, drawn from the considerations of human rights and utilitarianism, will need to be invoked for a full privacy theory.

The paper makes several contributions toward vindicating social conceptions of privacy as useful for understanding and guiding privacy policy:

- To survey a variety of social conceptions of privacy
- To add to these social conceptions by formulating a notion of harm to social contexts
- To show how familiar privacy restrictions have a basis in this notion of contextual harm
- To encourage the greater use of assessments of contextual harm in evaluating new information uses

II. PRIVACY AS AN ELEMENT OF SOCIAL STRUCTURE

A. Traditional Privacy Frameworks

One way to think about privacy is as a fundamental human right. In this rights-based way of thinking, privacy embodies aspects of human dignity. Respecting privacy is a way to affirm the value of individual autonomy and independence from the intrusions of state and society.[11] The traditional fair information practices implement this human rights-based approach to privacy.[12]

Lending support to this approach is the fact that privacy rights are established in various instruments of international and European human rights law.[13] In accordance with these international and European legal instruments, the European Data Protection Directive from 1995 implements this fundamental human right to privacy.[14] The

---

[11] EDWARD J. BLOUSTEIN, PRIVACY AS AN ASPECT OF HUMAN DIGNITY, *reprinted in* EDWARD J. BLOUSTEIN, INDIVIDUAL AND GROUP PRIVACY 1-47 (2d ed. 1978).

[12] *See* ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2016), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf [https://perma.cc/692V-SZEW]. For a complete list of fair information practices, see MEMORANDUM FROM THE DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE ON THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf [https://perma.cc/BR93-25S2].

[13] *See* G.A. Res. 217 (III) A, at art. 12, Universal Declaration of Human Rights (Dec. 10, 1948), http://www.un.org/en/documents/udhr/ [https://perma.cc/G8CR-3BAQ]; G.A. Res. 2200A (XXI), at art.17, International Covenant on Civil and Political Rights (Mar. 23, 1976), http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf [https://perma.cc/4QXN-UWK2]; European Convention on Human Rights, art. 8(1) (Sept. 3, 1953), 87 U.N.T.S. 103, http://www.echr.coe.int/Documents/Convention_ENG.pdf [https://perma.cc/Q9Q8-PGC3]; Treaty on the Functioning of the European Union, art. 16, 2012 O.J. (C 326) 47, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN [https://perma.cc/PGQ8-S76N]; Charter of Fundamental Rights of the European Union, art. 7, 8, 2000 O.J. (C 364) 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF [https://perma.cc/DAA8-MARK].

[14] Under Article 1(1) of the Directive, the objective of the Directive is the protection of "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." Council Directive 95/46/EC, art. 1(1), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en [https://perma.cc/5NBL-5A6D] (on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

new General Data Protection Regulation continues this objective of protecting the fundamental right to privacy.[15]

A second way of thinking about privacy is as the prevention of harm. A number of privacy scholars and practitioners have developed this harm framework including Posner,[16] Beales and Muris,[17] MacCarthy,[18] Wittes,[19] and Cate.[20] They all share the idea that privacy policy should focus on the prevention of specific, tangible harm to individuals and classes of individuals. The harm framework derives from the utilitarian tradition that sees utility or welfare as the major guide to public policy.

Privacy as the prevention of harm relies on a notion of harm. The conceptual resources needed to flesh out this notion of harm are already present in the Federal Trade Commission's notion of unfairness. It suggests thinking of an act or practice as harmful when "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[21]

This test has concentrates on aggregated harm to individuals, and suggests at least a qualitative cost-benefit test. It allows small individual level harms to be aggregated into a large quantitative harm. It is probabilistic and allows a substantial risk of harm to count as harmful. And it recognizes that every act or practice has the potential

---

[15] General Data Protection Regulation, *supra* note 5.

[16] *See* Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978).

[17] *See* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109 (2008).

[18] *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 425 (2011).

[19] *See* BENJAMIN WITTES, BROOKINGS INSTIT., DATABUSE: DIGITAL PRIVACY AND THE MOSAIC (Apr. 1, 2011), https://www.brookings.edu/research/databuse-digital-privacy-and-the-mosaic/ [https://perma.cc/8WTZ-9T8J].

[20] Fred Cate, *Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 343 (Jane K. Winn ed., 2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972 [https://perma.cc/FVZ5-XMT6].

[21] Federal Trade Commission Act, 15 U.S.C. § 45(n) (2006).

for positive consequences that need to be weighed before a judgment is made that the act or practice is harmful.[22]

B. Introduction to Privacy as an Element of Social Structure

In contrast to these traditional approaches, there is a family of theories that treat privacy as an element of social structure. This social conception of privacy is not meant to replace the familiar rights-based approach and the harm framework, but to supplement these traditional approaches and to draw attention to an important and sometimes neglected aspect of privacy, namely, its role in constituting and implementing group purposes, values and objectives.

A crucial part of this approach is the recognition that in many cases, public policy or law does not create privacy; it is often a pre-existing creature of social life and its requirements can be supported or suppressed by public policy and law. Privacy norms limit the observability of people when they are engaged in specific social practices; these norms exist in order to allow these social practices to flourish and derive a part of their justification from playing this social role.

Sometimes transparency of social practices is to the good, but often it is destructive of the goals, purposes and ends of the social practice in question. Privacy norms function to cloak social practices in those cases where observation would have harmful effects on the social practice itself.

This social conception of privacy is in sharp contrast to the individualist conception that rights-based theories and utilitarian theories share. In thinking of privacy as a human right, the idea is that privacy protects individuals from intrusions by society and state. It is a keep-out sign whereby individual autonomy and dignity can be preserved even against the demands of the welfare of society as a whole. For utilitarians, privacy is a personal preference that varies randomly in society. Some people are willing to share; others are not; still others will share depending on the purposes. It is a matter of individual taste.

The social conception of privacy brings privacy into the world of everyday life by thinking of it as vindicating social practices; it is not a way to withdraw from society, but a social norm that allows people to communicate and interact to perform their needed tasks in society.

---

[22] For a further discussion of this notion of harm, see MacCarthy, *supra* note 18.

Rather than serve as an obstacle to the achievement of public purpose or as a random idiosyncratic matter of individual taste, privacy performs essential social functions.[23]

An important concept in thinking of privacy as an element of social structure is the notion of a social norm. A social norm is a rule of conduct that governs the way people interact with each other in various parts of social life. The function of norms is to resolve problems of social interaction. They do this in several ways:

- imposing "a significant social pressure for conformity and against deviation;"[24]
- instilling a "belief by the people concerned in their indispensability for the proper functioning of society;"[25]
- by privileging norms in the common and expected clashes between the dictates of norms "on the one hand and personal interests and desires on the other."[26]

Theories of privacy as an element of social structure share the idea that privacy norms function in much the same way as all norms do to resolve problems of social interaction.

C. Nissenbaum

Nissenbaum's contextualist theory of privacy arises out of a communitarian approach to ethics and political philosophy. This style of moral theory privileges tradition, socially determined virtues and social norms as the basis of morality. Many communitarians are hostile to privacy since they view it as an attempt to impose individualistic rights against the common values of the community or

---

[23] FERDINAND DAVID SCHOEMAN, PRIVACY AND SOCIAL FREEDOM 8 (Cambridge Univ. Press 1992) (privacy "facilitates association with people, not independence from people.").

[24] Cass Sunstein, *Where do Norms Come From? A Review of The Emergence of Norms by Edna Ullmann-Margalit*, THE NEW RAMBLER (1978), http://newramblerreview.com/book-reviews/philosophy/the-emergence-of-norms [https://perma.cc/6MFU-G8HR].

[25] *Id.*

[26] *Id.*

to block the use of shaming and other techniques of social control to maintain public values and morals.[27]

Nissenbaum turns this communitarian idea on its head and sketches a view of privacy as informational norms whose widespread acceptance is essential to the integrity of different social contexts. Socio-technical systems that dissolve embedded context-relative social norms of information flows are seen as problematic. One function of privacy policy is to provide the legal resources for defending the integrity of social contexts against the tendency of new technological possibilities to undermine information norms that are essential to these social contexts.

This social conception of privacy does not articulate and defend a set of abstract principles that can be used universally to assess information flows. Privacy is not an autonomous legal or philosophical enterprise. It is embedded in the daily life and activity of people engaged in social pursuits. When a new socio-technical practice arises that changes information flows, the key assessment that needs to be made is not whether the new practice violates an abstract pre-defined right to privacy or whether it advances an abstract notion of human welfare, but whether the new practice is consistent with the ends, goals, and purposes of the context in which it is used. Privacy controversies arise when the new practice violates an entrenched social norm of information flow and adversely affects the ends, goals and purposes of the context in which it arises.

Nissenbaum's key idea is that privacy is a right to an appropriate flow of information, where appropriate is defined by the social context in which the information is generated, disclosed and used.[28] She develops the notion of a social context in sufficient detail so that it can be applied to a wide range of phenomenon.

This allows her to define contextual integrity as that which is preserved when informational norms are respected and that which is violated when informational norms are breached.[29] She notes, "[t]here is a strong kinship between contextual integrity and the concept of

---

[27] *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999).

[28] HELEN NISSENBAUM, PRIVACY IN CONTEXT 127 (2009) (the key insight of her view is that privacy is not defined by the notions of secrecy or control, but by the notion of context-dependent informational norms).

[29] *Id.* at 140.

reasonable expectations."[30] Indeed, it is a concept "rooted in convention, habit and custom."[31]

In this view, privacy is essentially related to entrenched transmission norms involving personal information. These transmission norms impose constraints on the flow of information by setting out the terms and conditions under which transfers of information ought or ought not to take place.[32]

For instance, the transmission principles under which information is transmitted in the context of an exchange between close friends are different than the transmission principles in a medical context. Intimate sharing of intimate details of personal life are expected to be mutual in the context of friendship, but would be totally out of place in a medical context.[33]

This approach is enormously appealing. It provides an intuitive and comprehensive way to think about and analyze privacy issues. Its great strength is in understanding why improper disseminations or uses of information produce the sense of outrage they do. People understand why violations of entrenched norms of behavior can produce widespread hostile reactions. Bringing this insight to bear on privacy issues illuminates many of the puzzles that have concerned privacy advocates, analysts, scholars and policy makers. People have such strong reactions against privacy intrusions, not because of their subjective views and idiosyncratic preferences about information flows, but because privacy intrusions work against widely accepted, well understood, entrenched social norms.

D. Merton

Robert Merton provides an account of privacy as an element of social structure.[34] The key idea is that privacy plays an essential social function:

---

[30] *Id.* at 162.

[31] *Id.* at 165.

[32] *Id.* at 145.

[33] *Id.*

[34] ROBERT MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 395-433 (1968).

> What is sometimes called 'the need for privacy' – that is, insulation of actions and thoughts from surveillance by others – is the individual counterpart to the functional requirement of social structure that some measure of exemption from full observability be provided for . . . "Privacy" is not merely a personal predilection; it is an important functional requirement for the effective operation of social structure.[35]

The important insight is that privacy is not simply a personal preference people happen to have. Nor is it a result of accidental developments in history or culture. Rather, for various social structures there is a functionally optimal degree of visibility. [36]

Privacy, "insulation of actions and thoughts from surveillance by others," improves the operation of social structure by varying the level of observability depending on the needs of the social structure itself, not on the personal preferences or needs of individuals. Privacy needs of individuals do not explain social norms of privacy. Rather the causation runs the other way: "resistance to full visibility of one's behavior appears . . . to result from structural properties of group life."[37]

In particular, role-expectations of social life need to provide some leeway for individual differences and circumstances, since role definitions cannot be specified to cover all possible personality types and situations. In this way, the "antipathy toward having one's every activity subject to observation" allows for individual variation in performing group roles.

Privacy norms allow sufficient flexibility for individual differences and give social space for tolerated evasions of norms. In addition, a restriction on the flow of information out of the social context in which it is created allows needed communication to take place within the context. For instance, the social norm that communications in classrooms are privileged maintains "a degree of autonomy for the

---

[35] *Id.* at 429.

[36] "[W]e are led to the idea that differing social structures require, for their effective operation, differing degrees of visibility. Correlatively it is being suggested that differing social structures require arrangements for insulation from full and uninhibited visibility if they are to function adequately: arrangements which, in the vernacular, are described as needs for privacy, or as the importance of secrecy . . ." *Id.* at 398.

[37] *Id.* at 397.

teacher." [38] Confidentiality rules in law, medicine, teaching and the ministry have "the same function of insulating clients from ready observability of their behavior and beliefs . . ."[39]

Merton's sociological functionalism that focuses on privacy as an element of social structure provides a rich and promising framework for thinking about issues of privacy policy and law.

E. Foucault

Foucault's work on the social effects of constant surveillance provides another way of examining the social role played by privacy.[40] His major contribution to privacy theory is his analysis of the behavioral and attitudinal effects of Bentham's prison reform proposal of a "Panopticon." But behind that analysis is an implied social role of privacy as a way to protect individuals and groups from external social control by modern and contemporary "disciplinary" institutions.

The social institution Foucault analyzes is a "Panopticon." The key element of such an institution is to:

> . . . place a supervisor in a central tower and . . . shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy . . . . the cells of the periphery . . . are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible. He is seen, but he does not see; he is the object of information, never a subject in communication . . . in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen.[41]

This physical arrangement has a social purpose. In addition to saving on the number of guards and other supervisory personnel, the ability of a single overseer to keep track of numerous individualized

---

[38] *Id.* at 429. *See also* Sweezy v. New Hampshire, 354 U.S. 234 (1957) (upholding the autonomy of the teacher in the classroom).

[39] MERTON, *supra* note 34, at 429.

[40] MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 195 (Alan Sheridan trans., 1977).

[41] *Id.*

inhabitants of the institution allows the rules and norms of the institution to fully penetrate minds of the inmates and guide their behavior without the need for explicit coercion.

Foucault's concern is with "disciplinary power from the beginning of the nineteenth century in the psychiatric asylum, the penitentiary, the reformatory, the approved school and, to some extent, the hospital."[42] The lack of privacy, the full observability of all aspects a person's behavior and conduct, "constant surveillance" is essential to this disciplinary power.

One aspect of this control is the way in which other social relationships are abolished. No social practice, group or context stands between the isolated individual and the controlling disciplinary institution. The group has been broken into isolated atomic parts; the collective effect of social exchanges ". . . is abolished and replaced by a collection of separated individualities."[43] Foucault sees that privacy has the social role of allowing the formation and maintenance of social relationships that will act as intermediary, protective institutions shielding thought and attitude from controlling visibility.

Foucault emphasizes this connection between individualized visibility and power by noting "the major effect of the Panopticon . . . (is) . . . to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power."[44] Visibility itself controls behavior, for ". . . it is not necessary to use force to constrain the convict to good behaviour, the madman to calm, the worker to work, the schoolboy to application, the patient to the observation of the regulations."[45]

Why? Because the person "who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection."[46]

Constant surveillance provides for "the basic functioning of a society penetrated through and through with disciplinary

---

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

mechanisms."[47] Surveillance is "a functional mechanism that must improve the exercise of power by making it lighter, more rapid, more effective, a design of subtle coercion."[48]

Many privacy theorists have used Foucault's insights on the effects of observability to critique contemporary society. Oscar Gandy warned of the dangers of a society in which people were continuously organized and reorganized into different statistical categories for the purpose of marketing and business decisions.[49] The philosopher Jeffrey Reiman identified four risks from a modern version of a panopticon, all of which are threats to the free exercise of individual autonomy.[50] In Julie Cohen's view in a panopticon without privacy protection there is no zone for autonomous self-development, and the beliefs, desires and attitudes of individuals under constant surveillance are more likely to track the mainstream and expected.[51] Paul Ohm has warned of the dangers of a panopticon he calls a "data base of ruin, a complete accounting of a person's life which would provide an adversary with sufficient information to discredit him or her and significantly degrade his or her life prospects."[52]

All four thinkers focus on how the disciplinary function of observability can harm individuals. Observation can be mistaken and discriminatory, it can limit individual freedom and autonomy and it can expose us to tangible personal harm. But this focus on individual harm misses the key insight of Foucault's analysis: by stripping people down into nothing but isolated individuals the mechanism of observability displaces intermediate social practices, prevents people from engaging in them, and so allows the substitution of the norms of disciplinary institutions for the norms of group practice.

---

[47] *Id.*

[48] *Id.*

[49] OSCAR GANDY, THE PANOPTIC SORT 200-01 (Herbert I. Schiller ed., 1993).

[50] Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA HIGH TECH. L.J. 34 (1995).

[51] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012).

[52] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

The key point is that the presence or lack of privacy has social implications. The absence of privacy protections functions to reinforce certain mechanisms of social control; the presence of these protections functions to create a society in which power is less centralized and dispersed and in which social practices themselves can provide an insulation against external social control.

F. Bloustein

Bloustein sets out a social theory of privacy in his exploration of the notion of group privacy as the "right to huddle."[53] In his view, group privacy contrasts with the familiar individual right to be left alone: "The right to be left alone protects the integrity and the dignity of the individual. The right to associate with others in confidence . . . assures the success and integrity of the group purpose."[54]

Bloustein recognizes the role of group privacy as an essential element of social structure that varies with the nature and purpose of different groups,[55] and "covers the large, formal organization, as well as the relatively informal relationship, and the whole range of intermediate variations in size, duration, and formality."[56]

Bloustein notes that law does not create group privacy practices. They have a history, tradition and basis in social practice that precedes any legal recognition and they persist through a variety of non-legal mechanisms.[57] We will see how the law reinforces social privacy norms in the next section on witness privileges.

---

[53] EDWARD J. BLOUSTEIN, GROUP PRIVACY: THE RIGHT TO HUDDLE, *reprinted in* EDWARD J. BLOUSTEIN, INDIVIDUAL AND GROUP PRIVACY 123-186 (2d ed. 1978).

[54] *Id.* at 181.

[55] "Confidentiality of communication in one's associations serves different purposes depending on the nature of the association . . . what they have in common is that, in each confidentiality serves to assure the success and preserve the integrity of the association." *Id.* at 181.

[56] *Id.* at 126.

[57] "[M]ost confidences are maintained without any reference to law at all. Among other factors, a sense of good faith, the fear of reprisal or loss of face, traditional practice, religious or ethical compunctions and intricacies of bureaucratic or organizational structure are important to the support of a system of confidences. Law acts as only one influence among many." *Id.* at 127.

G. Post

Robert Post develops a rich social theory of privacy in his analysis of various privacy torts.[58] His key idea is that the privacy tort "safeguards rules of civility that in some significant measure constitute both individuals and community."[59]

For Post the privacy tort of intrusion rests on a showing that the intrusion would be "offensive to any person of ordinary sensibilities" or "would be highly offensive to a reasonable person. "[60] According to Post, the privacy tort builds upon a pre-existing social norm and finds a basis for compensation in the fact that the norm has been violated, regardless of the actual specific mental suffering of the plaintiff. The tort ". . . rests on the premise that the integrity of individual personality is dependent upon the observance of certain kinds of social norms."[61]

Post argues that these social norms are themselves constitutive of human personalities. To be a person is to be deserving of certain patterns of deference and demeanor, Post argues, quoting sociologist Erving Goffman.[62] To violate those patterns is not to do a person physical damage, nor is it to inflict a psychological damage specific to that person's personality, attitude, or feelings. People whose privacy has been invaded have been denied respect, and consequently their status as persons to whom respect is due has been questioned.

Post calls the privacy rules involved "civility rules" and the personality protected by them the "social personality." These civility rules are constitutive of communities. They "give normative shape and substance to the society that shares them . . . [they] . . . define the very 'community' which the 'reasonable person' inhabits."[63]

---

[58] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, CAL. L. REV. (1989), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1210&context=fss_papers [https://perma.cc/2GV6-U8FR].

[59] *Id.* at 959.

[60] *Id.* at 960.

[61] *Id.* at 963.

[62] *Id.* at 962-63 (quoting Erving Goffman, *The Nature of Deference and Demeanor*, *in* INTERACTION RITUAL: ESSAYS ON FACE-TO-FACE BEHAVIOR 47, 84-85, 90-91 (1967)).

[63] *Id.* at 964.

These civility rules have their life independently of law. Indeed, law can and should recognize only some of them.[64] However, the social role of privacy, as embodied in privacy torts, is to uphold pre-legal social norms of civility that "define the substance and boundaries of community life."[65]

He laments the loss of the conception of privacy as essential to our common life and warns about the futility of trying to find a fully adequate theory of privacy in the language of rights and utilitarianism:

> And we are thus led to attempt to rationalize the value of privacy, to discover its functions and reasons, to dress it up in the philosophical language of autonomy, or to dress it down in the economic language of information costs. But this is to miss the plain fact that privacy is for us a living reality only because we enjoy a certain kind of communal existence.[66]

H. Regan

In her groundbreaking study of privacy, Priscilla Regan developed nuanced social conceptions of privacy.[67] For her, privacy has important social aspects because it has social value as a common value, a public value, and a collective value.[68]

Regan views privacy as a "common value" in that it is not an idiosyncratic personal belief but a widely shared social norm. This conception of privacy as a shared, common value converges with Nissenbaum's view that privacy is a context-dependent entrenched social norm. Regan finds evidence that we have shared views on the

---

[64] "For obvious reasons, however, the common law can maintain only a small subset of these norms. The law itself claims to enforce only the most important of them, only those whose breach would be "highly offensive." *Id.* at 975.

[65] *Id.* at 1008.

[66] *Id.* at 1009.

[67] *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225-227 (1995).

[68] Priscilla M. Regan, *Privacy and the Common Good: Revisited*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 50 (Beate Roessler & Dorota Mokrosinska, eds., 2015).

importance of privacy from the widespread negative reactions to intrusive government surveillance and information collected through social networking sites.[69]

Regan argues that privacy is a "public value" in two ways. First, it is instrumentally important for protecting free speech rights and from a controlling government's power. Second, the public establishes a social sphere where individuals can engage in political discourse about controversial issues of collective importance. This is done as part of a civic commitment to the common good – without seeking to advance their own social or economic interests.

Finally, Regan argues that privacy has an economic "collective value." Privacy is an economic good that could, in principle, be bought and sold in the marketplace, but for a variety of reasons, the marketplace will not produce a socially optimal amount of the good. [70]

I. Steeves

Steeves seeks to recover the social value of privacy, which she states has been missing from both theoretical discussions and policy practice. Steeves reacts strongly against the definition of privacy as purely the individual's right to control information about oneself that derives from Alan Westin's pioneering work. In a comprehensive survey that covers Mead, Altman and Westin, Steeves extracts a number of insights concerning the function that privacy plays in social relationships.[71]

One of the most important functions is to create socially necessary boundaries between the different social roles we play:

> . . . privacy . . . allows us to perform one role—as wife or mother—separate and apart from other roles—as teacher or policy maker, for example . . . surveillance is problematic precisely because it collapses the boundaries between roles and makes the individual

---

[69] *Id.* at 58.

[70] *Id.* at 62-63.

[71] *See, e.g.*, Valerie Steeves, *Reclaiming the Social Value of Privacy*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 191-208 (Ian R. Kerr, Valerie M. Steeves & Carole Lucock, eds., 2009).

> accountable for all her actions, independent of the context or the role she is playing.[72]

Steeves generalized this into a definition of privacy as "the boundary between self and other that is negotiated through discursive interaction between two or more social actors."[73] Thinking of privacy as an element of social interaction would avoid the legalistic emphasis on information flows. For example, use of this definition has inhibited hospital officials from passing on a patient's religious affiliation to the hospital chaplain without express written consent from the patient.

J. Benkler

Benkler relies upon a social theory of group privacy in his discussion of the whistleblower's defense.[74] In contrast to Merton and Bloustein who view group privacy as performing a valuable social function, Benkler thinks of group secrecy as a way for organizations to avoid public accountability. His theme is that ". . . secrecy insulates self-reinforcing internal organizational dynamics from external correction."[75]

Keeping group secrets enables the group not only to achieve its purposes, but also to cover up its mistakes. His advocacy for a new whistleblowing law takes place against the background of a social systems approach to information within organizations. For him groups, which he calls, "organizations," function using norms, which he calls "institutions," to form systems of interaction that have a certain independence with respect to the outside world. Norms of "secrecy" or "transparency" regulate the level of independence and autonomy that these organizations can maintain.[76]

---

[72] *Id.* at 205 (Steeves immediately draws the connection between this somewhat abstract sociological point about role boundaries and a pressing privacy policy issue, namely, a "society in which Facebook pictures are used by employers to decide whether or not to hire someone").

[73] *Id.* at 206.

[74] *See, e.g.*, Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 HARV. L. & POL'Y REV. 281 (2014).

[75] *Id.* at 285.

[76] *Id.* at 287-88.

Thus, an organization such as an intelligence agency can use secrecy ". . . to segment information flows about its structure and functions to allow it to project power in other systems and resist their incursions."[77] Accountability leaks or acts of whistleblowing perform an opposing but valuable system function, namely, correction of inevitable systemic mistakes.[78]

The fact that Benkler emphasizes the social function of transparency rather than group privacy should not fool us into thinking that he has no sense of the social function of group privacy. He is aware that it has social consequences and plays a role in the social life of organizations and systems. His view, however, is that the level of visibility in national security organizations is far less than Merton's optimum. Of course, group privacy helps organizations achieve group purposes, but too much secrecy means the loss of the accountability function that is also a key element in social structure.

III. THE ROLE OF WITNESS PRIVILEGES IN PRESERVING PRIVACY NORMS

So far, we have reviewed different ways in which privacy can be thought of as an element of social structure. We are now able to examine how law and public policy should treat privacy norms that function to protect the integrity of social contexts using the example of witness privileges.

In general, law does not disturb social norms. It neither requires obedience to social norms, nor forbids it. In the case of confidentiality norms, ". . . the law rarely requires people to break their confidences with one another; indeed, the law protects and favors confidences in most circumstances."[79]

Sometimes, however, confidentiality norms come into conflict with the normative requirements of other parts of a social system. This is often the case with conflicts between norms of confidentiality and the requirements of the legal system to get at the truth of a matter in order to dispense justice. To get our bearings, we start with Bentham's famous defense of the privacy of the confessional.

---

[77] *Id.* at 288.

[78] *Id.* at 289.

[79] BLOUSTEIN, *supra* note 53, at 136.

A. Bentham and the Confidentiality of the Confessional[80]

It is well known that Bentham did not believe in the attorney client privilege. He thought it provided a cloak that could only hide villainy and he thought that lawyers should be required to testify about matters communicated to them in confidence by their clients.[81]

Bentham reached an entirely different conclusion in the case of the confidentiality of the confessional. The argument for forcing priests to disclose the contents of confessions is that it would increase the evidence available in court. But would it over the long term?

Bentham's argument is this: once it is known that Catholic priests must disclose the contents of confessions in court proceedings, Catholics will stop disclosing in confession anything that could be used against them in court, effectively ending the practice of confession. But this accomplishes no worthwhile purpose, since after an adjustment period there would be no increase in court evidence. The only increase in evidence available in court would come during a transition period, when people learn to adjust to the new reality, by avoiding full disclosure in the confessional.[82]

So, there is nothing to be gained in the long run from allowing confessional evidence to be used in court proceedings. On the negative side, Bentham argues, allowing confessional evidence in court is equivalent to banning the practice of confession and so would be

---

[80] JEREMY BENTHAM, RATIONALE OF JUDICIAL EVIDENCE 586, 588 (Hunt & Clarke eds., 1827).

[81] *See* RONALD GOLDFARB, IN CONFIDENCE: WHEN TO PROTECT SECRECY AND WHEN TO REQUIRE DISCLOSURE 59 (2009).

[82] "Suppose it is an established, and thence a known rule of procedure, that a catholic priest is not exempted from the obligation of disclosing . . . statements made to him . . . by a . . . penitent . . . in the character of self-prejudicing (including self-incriminating) evidence . . . in or for the use of a court of justice . . . What would be the consequence? – That, of that quantity of confessorial evidence which is now delivered in secret for a purpose purely religious, a certain proportion (it is impossible to say what, but probably a very considerable one) would not be so delivered: would be kept back, under the apprehension of its being made use of for a judicial purpose. The rule would operate as a prohibition upon all such confessions for the spiritual purpose, as would be applicable to the temporal purpose: and the penalty would be, whatever consequence of a penal or otherwise burthensome nature might be expected to flow from the decision which such testimony would warrant, and would therefore be calculated to draw forth." BENTHAM, *supra* note 80, at 587.

inconsistent with freedom of religion, putting an intolerable burden on penitent and confessor alike.[83]

In effect, Bentham says, the rule allowing confessor evidence would threaten the institution of the confession and ". . . this institution is an essential feature of the catholic religion, and . . . the catholic religion is not to be suppressed by force."[84]

For the purpose of analyzing contextual harm, it is important to keep this example and style of argumentation before us as a paradigm case and to keep as a theme the idea that allowing information out of a context for a different purpose can harm the social practices characteristic of that context

B. Witness Privileges in General

We now turn to the consideration of witness privileges under U.S. law. Witness privileges are exceptions to the general rule that all citizens have an obligation to contribute to the search for truth in court proceedings. The general obligation to tell what one knows is straightforward: If people know something that can help advance a plaintiff's or defendant's cause or to convict or acquit defendants in a criminal trial, they should be required to produce that information in open court so that justice can be served.[85] In general, pledges of

[83] "[W]ith any idea of toleration, a coercion of this nature is altogether inconsistent and incompatible. In the character of penitents, the people would be pressed with the whole weight of the penal branch of the law; inhibited from the exercise of this essential and indispensable article of their religion; prohibited, on pain of death, from the confession of all such misdeeds as, if judicially disclosed, would have the effect of drawing down upon them that punishment; and so, in the case of inferior misdeeds, combated by inferior punishments . . . To confessors, the consequences would be at least equally oppressive. To them it would be a downright persecution . . . it would be an order to violate what is by them numbered amongst the most sacred of religious duties." *Id.* at 588.

[84] *Id.* at 590.

[85] "For more than three centuries it has now been recognized as a fundamental maxim that the public . . . has a right to every man's evidence. When we come to examine the various claims of exemption, we start with the primary assumption that there is a general duty to give what testimony one is capable of giving, and that any exemptions which may exist are distinctly exceptional, being so many derogations from a positive general rule." Jaffee v. Redmond, 518 U.S. 1, 9 (1996) (citations omitted).

secrecy are insufficient to withhold information in court proceedings.[86]

Despite this general rule in favor of full disclosure in court proceedings, U.S. law recognizes a series of witness privileges. A uniform code of rules of evidence containing nine specific witness privileges was first proposed in 1972, but it never became law.[87] Instead, in 1975 Congress passed a general rule of privilege under Rule 501, providing that the common law as interpreted on a case-by-case basis "in the light of reason and experience" is the touchstone for witness privileges.[88]

The Supreme Court constructed a test that calls for granting a witness privilege when the privilege serves "significant public and private interests" and the "likely evidentiary benefit that would result from the denial of the privilege is modest."[89] The public served by

---

[86] "[N]o pledge of privacy nor oath of secrecy can avail against demand for the truth in a court of justice." GOLDFARB, *supra* note 81, at 19 (quoting JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW (1905)).

[87] In 1972, the Supreme Court approved a uniform code of rules of evidence to be used in federal court and transmitted these rules to Congress. *See* 56 F.R.D. 183 *(*1972*)*. An Advisory Committee appointed by the Court drafted the rules over a period of seven years and the Judicial Conference approved them. *See* Paul Rothstein, *The Proposed Amendments to the Federal Rules of Evidence*, 62 GEO. L.J. 125, 125 (1973); *see also* Trammel v. United States, 445 U.S. 40, 47 (1980); *Jaffee*, 518 U.S. at 8 n.7. The code contained nine specific rules relating to the privilege of certain witnesses to refrain from testifying in court proceedings including and limited to: a privilege for those reports required under state or federal statute, when that statute grants a privilege; a lawyer-client communications privilege (Rule 503); a psychotherapist-patient communications privilege (Rule 504); a privilege of an accused to prevent his spouse from testifying against him in a criminal proceeding (Rule 505); a privilege covering communications to clergymen (Rule 506); a privilege to refuse to disclose the tenor of one's lawful vote (Rule 507); a trade secrets privilege (Rule 508); and a privilege covering secrets of state and other official information and a privilege covering the identity of an informer (Rule 510). This list of privileges was exclusive; additional privileges could be recognized by Federal courts only if required by the Constitution, a further act of Congress, or new evidence rules adopted by the Supreme Court. *See* FED. R. EVID. 501–513 (proposed); 56 F.R.D. 230–261. These nine privilege rules leave out a general physician-patient privilege, a spousal communications privilege, and a journalist's privilege. *See* Rothstein, *supra* note 87, at 129.

[88] "The common law — as interpreted by United States courts in the light of reason and experience — governs a claim of privilege unless any of the following provides otherwise: The United States Constitution; a federal statute; or rules prescribed by the Supreme Court." FED. R. EVID. 501. The legislative history of the Congressional action adopting Rule 501 stated that it "should be understood as reflecting the view that the recognition of a privilege based on a confidential relationship . . . should be determined on a case-by-case basis." S. REP. NO. 93–1277, at 13 (1974).

[89] *Jaffee*, 518 U.S. at 11.

witness privileges relate to the preservation and fostering of social relationships whose proper functioning serves society. Hence, there are "privileges between priest and penitent, attorney and client, and physician and patient . . . (that) . . . are rooted in the imperative need for confidence and trust."[90] Sissela Bok makes a similar point in regard to the premise that the witness privilege rests on the "benefits of confidentiality to those in need of advice, sanctuary, and aid, and in turn to society."[91]

There are potentially other justifications for witness privileges, such as preventing "psychological injury to those who shared their secrets" and preserving people's "autonomy and decisional privacy."[92] However, the key argument is social: what would happen to the social practice under consideration (legal practice, religious comfort, medical service, or psychological counseling), if the social norm of confidentiality inherent in these practices was breached and information given in confidence was made available in the very different context of court proceedings?

Respect for context and the need to avoid harm to a social context suggests that the law should recognize these privileges. Other considerations, however, must be taken into account before a final choice is made. Sometimes the issue is framed as the need for a

---

[90] "The priest-penitent privilege recognizes the human need to disclose to a spiritual counselor, in total and absolute confidence, what are believed to be flawed acts or thoughts and to receive priestly consolation and guidance in return. The lawyer-client privilege rests on the need for the advocate and counselor to know all that relates to the client's reasons for seeking representation if the professional mission is to be carried out. Similarly, the physician must know all that a patient can articulate in order to identify and to treat disease; barriers to full disclosure would impair diagnosis and treatment." *Trammel*, 445 U.S. at 51.

[91] "According to this premise, individuals benefit from such confidentiality because it allows them to seek help they might otherwise fear to ask for; those most vulnerable or at risk might otherwise not go for help to doctors or lawyers or others trained to provide it. In this way, innocent persons might end up convicted of crimes for lack of competent legal defense, and disease could take a greater toll among those ashamed of the nature of their ailment. Society therefore gains in turn from allowing such professional refuge, the argument holds, in spite of the undoubted risks of not learning about certain dangers to the community; and everyone is better off when professionals can probe for the secrets that will make them more capable of providing the needed help." SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 122 (1989).

[92] GOLDFARB, *supra* note 81, at 1, 19.

balance[93] or even a choice between the evil of "betrayal of confidence" and the evil of "suppression of truth."[94]

But this idea of balancing the harm to the context against the advantages of additional court testimony misstates the real question. As Bentham noted in the confessional case, when there really is harm to a social context, there is no additional court testimony at all. Once it is known that confidential information will be available in court if revealed in confidence, it will no longer be revealed in the first place, and the quantity of information available in court will be the same as if the privilege were granted. The real question is the extent of the risk that people will withhold information in specific social contexts in the absence of a privilege. Courts are really engaged in a kind of empirical risk assessment. They tend to grant the privilege when they think this risk is unacceptably high, and they tend to withhold the privilege when they think the risk is minimal or tolerable.

Next, we will consider several of these witness privileges to illustrate how the arguments for them rely on the notion of contextual harm. The examples are the psychotherapist-patient privilege, the attorney-client privilege, the spousal privilege, the journalist's privilege, the doctor-patient privilege, and the protection of genetic information. Common themes emerge from this consideration: the role of privileges in upholding social practices that further the public interest, the reasoning that upholds or rejects the privilege depending on the assessment of the risk of harm to the social practice by withholding the privilege, and the need for certainty and predictability about the contours of the privilege in order to assure its effectiveness.

---

[93] Wigmore, for example, sets out four criteria for a witness privilege: the communication must originate in a confidence; the sharing of confidences must be of the essence of the relationship; the relationship must be favored by public policy; and the injury which flows from the breach of confidence must be more significant to society than the loss of the testimony. BLOUSTEIN, *supra* note 53, at 133 (quoting J. WIGMORE, EVIDENCE § 2285 (J. McNaughton rev. 1961)) (the last criterion suggests that the injury to a social practice from compelled testimony would be compensated for by the greater quantity of truthful testimony in court. Bloustein makes a similar balancing point, saying, "in considering whether to grant a privilege, the law weighs the harm to the association from compelled testimony against the benefit afforded to our system of justice.").

[94] "[T]he definition of the privilege will express a value choice between protection of privacy and discovery of truth and the choice of either involves the acceptance of an evil - betrayal of confidence or suppression of truth." Geoffrey C. Hazard Jr., *An Historical Perspective on the Attorney-Client Privilege*, 66 CAL. L. REV. 1061, 1085 (1978).

C. Psychotherapist-Patient Privilege

People confide sensitive personal details of their lives to their counselors in order to receive professional guidance on their emotional lives and on the conduct of their personal relationships. The norm of confidentiality of the counselor-client relationship gives people the trust they need to disclose intimate information to professional counselors in order to receive this professional guidance.

The legal recognition of this norm as a witness privilege is relatively new because the psychotherapeutic context itself is relatively new. It wasn't until the 1950's that the practice of psychotherapy received widespread cultural acceptance. As more and more people looked for treatment and expected confidentiality, "powerful cultural forces were brought to bear on courts for the protection of this expanding form of treatment." By the mid-1970s, all fifty states had passed laws recognizing this privilege.[95]

In 1996, the privilege was subject to a Federal court challenge. A police officer named Redmond was accused in federal court of violating the constitutional rights of a person she killed in the line of duty. The police officer's professional counselor, a licensed social worker, refused to hand over her counseling notes as part of court evidence in the case. In *Jaffee v. Redmond*, the Supreme Court ruled that the "conversations between Redmond and her therapist and the notes taken during their counseling sessions are protected from compelled disclosure under Rule 501."[96] The court drew attention to the essential role confidentiality played in successful psychotherapy:

> Effective psychotherapy . . . depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. Because of the sensitive nature of the problems for which individuals consult psychotherapists, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason, the mere possibility of

---

[95] GOLDFARB, *supra* note 81, at 108. The quotation is from Goldfarb Kindle location 1343; the 50 states fact is from Goldfarb Kindle location 1376.

[96] Jaffee v. Redmond, 518 U.S. 1, 2 (1996).

> disclosure may impede development of the confidential relationship necessary for successful treatment.[97]

This conclusion was backed by empirical evidence from the American Psychological Association showing that absent confidentiality "the trust vital to the psychotherapeutic relationship is likely to be significantly impaired or destroyed."[98] Some people might still take advantage of the services of a psychological counselor, but the practice will be more limited and restricted than it otherwise would be, and indeed, might not be available for those who need it most.

The *Jaffee* Court reasoned the psychotherapist privilege "serves the public interest" by facilitating mental health of the citizenry, which is a public good "of transcendent importance."[99] Moreover, without a privilege, no new evidence is likely "to come into being. This unspoken 'evidence' will therefore serve no greater truth-seeking function than if it had been spoken and privileged."[100]

Finally, the *Jaffee* Court rejected a privilege that is subject to ad hoc case-by-case balancing, ruling that later evaluations of the need for confidentiality by a trial judge "would eviscerate the effectiveness of the privilege."[101]

D. Attorney-Client Privilege

The attorney-client witness privilege protects this confidential relationship from court disclosure because without it "clients would

---

[97] *Id.* at 10.

[98] Brief for the American Psychological Ass'n, as Amici Curiae Supporting Respondents at 14, Jaffee v. Redmond, 518 U.S. 1 (1996). The impairment of the psychotherapeutic relationship manifests itself in a number of ways: patients would find it difficult to talk or would discontinue therapy if told before the first session that they were not confidential; patients would be upset or angry if their confidences were revealed without permission; when patients are told that their therapist might be required to disclose their communications in court, their willingness to discuss sensitive topics declines markedly; fear of disclosure causes some patients to terminate the psychotherapeutic relationship threat of public disclosure deters people with emotional problems from seeking needed help in the first place. *See id.* at 14-15.

[99] *Jaffee*, 518 U.S. at 11.

[100] *Id.* at 12.

[101] *Id.* at 17.

not consult attorneys . . . ."[102] The attorney-client privilege has long been part of the common law, and its existence has not been the subject of any serious legal challenge. However, the scope of the privilege is defined by two Supreme Court cases. In *Upjohn Co. v. United States*, the Supreme Court clarified that the privilege extended to corporate lawyers.[103] In *Swidler & Berlin v. United States*, the Supreme Court ruled that the privilege continued after the death of the client.[104]

The *Upjohn* Court noted that the purpose of the privilege "is to encourage full and frank communication between attorneys and their clients, and thereby promote broader public interests in the observance of law and administration of justice."[105] The assistance of skilled attorneys "can only be safely and readily availed of when free from the consequences or the apprehension of disclosure."[106]

The *Swidler* Court notes that withdrawal of the privilege dos not increase the quantity of evidence available in court because without the privilege "the client may very well not have made disclosures to his attorney at all, so the loss of evidence is more apparent than real."[107]

---

[102] GOLDFARB, *supra* note 81, at 59 (he rejects this utilitarian defense of the privilege as "anecdotal, self-serving, and empirically unsupported.").

[103] Upjohn Co. v. United States, 449 U.S. 383, 386 (1981).

[104] Swidler & Berlin v. United States, 524 U.S. 399, 401 (1998).

[105] *Upjohn Co.*, 449 U.S. at 389. In *Trammel*, the Supreme Court described the rationale for the privilege this way, "[t]he lawyer-client privilege rests on the need for the advocate and counselor to know all that relates to the client's reasons for seeking representation if the professional mission is to be carried out." Trammel v. United States, 445 U.S. 40, 51 (1980).

[106] *Upjohn Co.*, 449 U.S. at 389 (quoting Hunt v. Blackburn, 128 U. S. 464, 470 (1888)). Geoffrey Hazard makes a similar point: "Total abolition would mean that an accused in a criminal case could not explain his version of the matter to his lawyer without its being transmitted to the prosecution. Defense counsel would become a medium of confession, a result that would substantially impair both the accused's right to counsel and the privilege against self-incrimination." Hazard, *supra* note 94, at 1062.

[107] *Swidler & Berlin*, 524 U.S. at 408 (citations omitted). Geoffrey Stone makes a similar point about the self-defeating nature of taking away the privilege: "If the client would not have disclosed this fact to his lawyer without the assurance of the privilege, then the prosecution loses nothing by not being able to learn the information from the lawyer, because without the privilege the lawyer wouldn't have known the information in the first place." Geoffrey Stone, *Democracy Demands a Journalist-Source Shield Law*, THE DAILY BEAST (Apr. 15, 2014), http://www.thedailybeast.com/articles/2014/04/15/democracy-demands-a-journalist-source-shield-law.html [https://perma.cc/FRY8-PNE5].

Finally, the *Upjohn* Court noted that the contours of the privilege must be predictable, since "[a]n uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all."[108] The *Swidler* Court agreed and for that reason rejected an after-the-fact balancing test.[109]

In summary, the public benefit derived from the attorney-client privilege is "the observance of law and administration of justice." This public benefit is obtained only by preserving the integrity of the professional relationship between lawyer and client. Preserving this relationship does not decrease the flow of evidence to the court because without it the disclosure to the attorney would never have been made in the first place. Finally, the contours of the privilege must be predictable, since an uncertain privilege is little better than no privilege at all.

E. Spousal Privilege

There are two versions of this privilege. The marital communication privilege provides that unwilling spouses cannot be compelled to disclose the contents of private communications with each other. The other privilege is a bar against spouses testifying against each other, even if one of them is willing to provide such testimony.

1. Marital Communication Privilege

The Supreme Court in *Wolfle* allowed a letter between spouses to be admitted into evidence because the husband had disclosed it to his

---

[108] *Upjohn Co.*, 449 U.S. at 393. Even though the extent of the privilege must be predictable, there must be some limits on the privilege, "for at minimum it is inadmissible that legal consultation be a cover for thuggery and theft." Hazard, *supra* note 94, at 1091. So, the privilege does not apply, for example, when "the legal service was sought or obtained . . . to commit or plan to commit a crime or a tort." *Id.* at 1063. The privilege also does not provide an automatic way for a party to withhold information from the court merely by revealing it to his lawyer. As the *Upjohn* Court put it: "The client cannot be compelled to answer the question, 'What did you say or write to the attorney?' but may not refuse to disclose any relevant fact within his knowledge merely because he incorporated a statement of such fact into his communication to his attorney." *Upjohn Co.*, 449 U.S. at 396 (citations omitted).

[109] "Balancing ex post the importance of the information against client interests, even limited to criminal cases, introduces substantial uncertainty into the privilege's application. For just that reason, we have rejected use of a balancing test in defining the contours of the privilege." *Swidler & Berlin*, 524 U.S. at 409 (citations omitted).

stenographer. But the *Wolfle* Court upheld the privilege itself because marital confidences are "so essential to the preservation of the marriage relationship as to outweigh the disadvantages to the administration of justice which the privilege entails."[110] The marital communications privilege "should be allowed only when it is plain that marital confidence cannot otherwise reasonably be preserved."[111]

In the 1951 *Blau* case, the Supreme Court ruled that the marital communications privilege protected a witness's refusal to disclose his wife's location to a grand jury, saying that the witness "obtained his knowledge of his wife's whereabouts by communication from her," that "marital communications are presumptively confidential" and the witness's "refusal to betray his wife's trust therefore was both understandable and lawful."[112]

In the 1981 *Trammel* case, the Supreme Court narrowed the prohibition against adverse spousal testimony and at the same time reaffirmed "the independent rule protecting confidential marital communications" whose purpose is "to protect information privately disclosed between husband and wife in the confidence of the marital relationship — once described by this Court as 'the best solace of human existence.'"[113]

In these decisions, the Court recognizes the social dimensions of the marital communication privilege. The damage to the institution of marriage would be substantial and lasting if spouses were required to reveal in court the contents of communications made to each other in confidence.[114]

---

[110] Wolfle v. United States, 291 U.S. 7, 14 (1934).

[111] *Id.* at 17.

[112] Blau v. United States, 340 U.S. 332, 333-34 (1951).

[113] Trammel v. United States, 445 U.S. 40, 51 (1980).

[114] The *Wolfle* Court also delineated some of the curious contours of the marital communication privilege, ruling "communications between husband and wife, voluntarily made in the presence of their children, old enough to comprehend them, or other members of the family within the intimacy of the family circle, are not privileged." *Wolfle*, 291 U.S. at 17. The rationale for protection one intimate relationship, but not the others is not clear.

2. Adverse Spousal Testimony

The evolution of the prohibition against adverse spousal testimony from *Hawkins v. United States*[115] to *Trammel v. United States*[116] illustrates the way in which law of witness privileges changes in social practices and reveals that the basis for a privilege is often an assessment of the risk of harm to a valuable social relationship.

The spousal privilege against adverse testimony began as a spousal disqualification, where a wife could not testify either for or against her husband since she was essentially the same legal person as the husband and his evidence for or against himself was inadmissible. By the 1950s, with the change in the social role of women, this disqualification was narrowed to a privilege that allowed one spouse to testify for the other, but barred adverse testimony unless both parties consented.[117]

In the 1958 *Hawkins* case, the Supreme Court rejected a modification of the two-party privilege that would allow one spouse to testify voluntarily against the other because "the law should not force or encourage testimony which might alienate husband and wife, or further inflame existing domestic differences."[118]

In a concurring opinion, however, Justice Stewart noted that this privilege was widely viewed as a "sentimental relic" and adherence to it was worship of an outdated tradition. The Court should do "more than indulge in mere assumptions, perhaps naive assumptions, as to the importance of this ancient rule to the interests of domestic tranquility."[119]

In 1980, the *Trammel* Court accepted the voluntary adverse spousal testimony privilege arguing "investing the privilege in the witness-spouse . . . furthers the important public interest in marital harmony without unduly burdening legitimate law enforcement needs."[120] The Court found that the "ancient foundations" for the

---

[115] Hawkins v. United States, 358 U.S. 74 (1958).

[116] *Trammel*, 445 U.S. at 46.

[117] *Id.*

[118] *Hawkins*, 358 U.S. at 79.

[119] *Id.* at 81 (Stewart, J., concurring). Justice Stewart concurred in part because of the difficulty of determining when a spouse was testifying voluntarily.

[120] *Trammel*, 445 U.S. at 53.

"sweeping" two-party consent privilege against adverse spousal testimony relating to the lesser social and legal status of women "have long since disappeared." Moreover, the two-party consent privilege did not in fact further the public interest in preserving the integrity of the marital relationship, since "when one spouse is willing to testify against the other in a criminal proceeding . . . there is probably little in the way of marital harmony for the privilege to preserve."[121]

F. Reporter's Privilege

The legal arguments surrounding the reporter's privilege also reflect our themes of the social importance of the practice to be protected, empirical assessment of the actual risk to that practice and a judgment that an uncertain privilege would not protect the practice.

Common journalistic practice is to maintain source confidentiality when needed. However, in 1972, the Supreme Court in *Branzburg v. Hayes* ruled that reporters have no right under the First Amendment or the common law to refuse to disclose informant information in grand jury proceedings.[122]

The reasoning in this case turns on the extent to which a privilege, absolute or qualified, is needed to protect the public interest in newsgathering. Society's interest in the reporter-informer relationship is "not in the welfare of the informant per se, but rather in creating conditions in which information possessed by news sources can reach public attention."[123]

The *Branzburg* Court considered the argument that if reporters are legally required to reveal confidential news sources, then "the source so identified and other confidential sources of other reporters

---

[121] *Id.* at 52.

[122] Branzburg v. Hayes, 408 U.S. 665 (1972). However, reporter shield laws in effect in many states and under consideration at the federal level provide legal protection for this journalistic practice.

[123] *Id.* at 727 (citing *Notes: Reporters and Their Sources: The Constitutional Right to a Confidential Relationship,* 80 Yale L.J. 317, 343 (1970)). *See also id.* at 737-38 (Stewart, J., dissenting) ("[T]his protection does not exist for the purely private interests of the newsman or his informant, nor even, at bottom, for the First Amendment interests of either partner in the newsgathering relationship. Rather, it functions to insure nothing less than democratic decision-making through the free flow of information to the public."). Bok makes a similar point: "And the help held to justify confidentiality about informants by police and journalists is not directed to individuals in need of relief at all, but rather to society by encouraging disclosures of abuses and crime." BOK, *supra* note 91, at 119-24.

will be measurably deterred from furnishing publishable information, all to the detriment of the free flow of information protected by the First Amendment."[124] But it rejected this argument on factual grounds, holding that "nothing before us indicates that a large number or percentage of all confidential news sources would in any way be deterred . . . ." by the absence of a reporter's privilege based on the First Amendment.[125]

In contrast, the dissent from Justice Stewart argued that the confidentiality of the relationship with a source ". . . is essential to the creation and maintenance of a newsgathering relationship with informants . . . ."[126] When grand juries can subpoena reporters to testify about their sources, these sources "become fearful of disclosing information" and the newsman "will cease to investigate and publish information about issues of public import . . ." Moreover, the ability to subpoena reporters will not increase the flow of information to the courts because informants will cease to reveal information to reporters and in the absence of any informant information to disclose "the newsman will . . . cease to be a useful grand jury witness."[127]

Justice Douglas agreed about the empirical effect of ending the privilege, arguing if a reporter ". . . can be summoned to testify in secret before a grand jury, his sources will dry up and the attempted exposure, the effort to enlighten the public, will be ended."[128]

The court had before it not only a blanket absolute privilege but also a qualified privilege that would permit compelled testimony only if certain conditions were fulfilled, including a "compelling need" for the testimony.[129] The majority rejected this qualified privilege as too uncertain to provide reassurance to any reluctant informants, arguing, "If newsmen's confidential sources are as sensitive as they are claimed to be, the prospect of being unmasked whenever a judge determines

---

[124] *Branzburg*, 408 U.S. at 680.

[125] *Id.* at 691. The *Branzburg* opinion also notes that lower courts had reached similar empirical conclusions in describing as "tenuous" and "indirect, theoretical, and uncertain" the argument that revealing this information to a grand jury would destroy the ability to gather news. *Id.* at 671, 674.

[126] *Id.* at 728.

[127] *Id.* at 746.

[128] *Id.* at 722.

[129] *Id.* at 742.

the situation justifies it is hardly a satisfactory solution to the problem.[130]

G. Confidentiality of Medical Records

Confidentiality rules for medical information are often justified on the basis of their utility in protecting certain social practices, namely the successful practice of medicine and the effective conduct of medical research.

The confidentiality of doctor-patient relationship is needed to protect the willingness of patients to disclose information to doctors for treatment. People do not expect their doctor to share their medical condition casually with friends and acquaintances or to use it for their own personal advantage. This confidential relationship is privileged, allowing medical personnel to refuse to testify in court because ". . . the utmost confidence between doctors and patients was necessary to ensure correct diagnoses."[131] The medical confidence is not absolute, however. Doctors are required to report a range of illnesses to public health officials, including venereal disease and the use of illegal drugs.[132]

The norm of medical confidentiality is as old as the Hippocratic Oath.[133] But the common law in the United States did not protect medical confidentiality. Beginning with New York in 1828, however, the states passed witness privilege laws in an attempt to ensure that

---

[130] *Id.* at 702. The court cites a 1970 law review article arguing that an uncertain and unpredictable qualified privilege would have a "general deterrent effect" and would "undermine significantly the effectiveness" of the privilege. It concluded that for the purpose of effectively protecting informants "only an absolute privilege would suffice." The court's objection to the privilege is empirical – neither the absolute nor the qualified privilege is needed to protect informants, but it accepts the argument that if informants were deterred form sharing information with reporters because of the prospect of later revelation in court, a qualified privilege would not protect them. Federal legislation establishing a reporter's privilege is also qualified holding that a reporter may refuse to testify unless a number of specific conditions apply. *See, e.g.*, discussion of H.R. 985, THE FREE FLOW OF INFORMATION ACT OF 2009, H.R. RES. 111-61, at 8 (2015).

[131] GOLDFARB, *supra* note 81, at 87.

[132] BLOUSTEIN, *supra* note 53, at 134.

[133] The oath reads as follows: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about." *See* GOLDFARB, *supra* note 81, at 87.

people sought treatment for diseases, a rationale based more on public health than on the idea that medical information is intrinsically sensitive.[134]

The traditional social norm of doctor-patient confidentiality is also protected by explicit regulation. The Department of Health and Human Services (HHS) established the medical Privacy Rule under the Health Insurance Portability and Accountability Act (HIPAA) so as to ". . . make the use and exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care."[135] The rule requires patient authorization for the use and exchange of health information unless it is for health care purposes or one of twelve specifically defined public benefit purposes.[136]

The rationale for the rule was the need to provide doctors with accurate information in order for patients to receive medical care.[137] HHS noted the existence of substantial concern among patients about the possible misuse of their health information.[138] The absence of a national privacy standard was adversely affecting the provision of health care. In one national survey, ". . . one-sixth of respondents

---

[134] These laws were aimed to "encourage people to seek medical care when needed, even for embarrassing or socially unacceptable diseases." GOLDFARB, *supra* note 81, at 87.

[135] Standards for Privacy of Individually Identifiable Information, 64 Fed. Reg. 59,924 (Nov. 3, 1999) (codified at 45 C.F.R. 164.512).

[136] Health care purposes are defined to include "treatment, payment and health care operations." No patient authorization is needed for these purposes because these purposes are within the medical context or are operations essential for the functioning of the medical context. The public benefit purposes are that justify release of medical information without patient consent are: Required by Law, Public Health Activities, Victims of Abuse, Neglect or Domestic Violence, Health Oversight Activities, Judicial and Administrative Proceedings, Law Enforcement Purposes, Decedents Cadaveric Organ, Eye, or Tissue Donation, Research, Serious Threat to Health or Safety, Essential Government Functions, Workers' Compensation. *See* DEP'T OF HEALTH & HUMAN SERVICES, SUMMARY OF THE HIPAA PRIVACY RULE (2003).

[137] "In order to receive accurate and reliable diagnosis and treatment, patients must provide health care professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives." *See* Standards for Privacy of Individually Identifiable Information, *supra* note 135, at 59,919.

[138] HHS found that patients wanted "to know that their sensitive information will be protected not only during the course of their treatment but also in the future as that information is maintained and/or transmitted within and outside of the health care system." *Id.*

indicated that they had taken some form of action to avoid the misuse of their information, including providing inaccurate information, frequently changing physicians, or avoiding care."[139]

Some have made the argument that medical confidentiality cannot be justified by the empirically false argument that without it people would avoid doctors.[140] According to this way of thinking, people will generally seek medical care regardless of whether their medical information is kept confidential because without medical care they will not recover from diseases. But this all or nothing way of thinking about the problem is mistaken. In emergencies, people will rush to a doctor and will usually disclose all to the attending physicians without bothering to calculate how much of this disclosure might come back to hurt them. But it is a public health problem when one out of every six patients is taking evasive action in their interactions with the health care system in order to avoid the misuse of their information. Medical confidentiality is one way to respond to evidence of a substantial decline in the utilization of the health care system.

The goal is the protection of public health and the confidentiality rules are based on the empirical assessment that without the rules public health would be impaired. The rule also modifies the extent of the confidentiality provided depending on the urgency of the competing public benefit. Thus, the rule generally permits disclosure of medical information for law enforcement purposes without patient consent.[141] However, disclosure is not permitted to law enforcement when the medical information disclosed in counseling or therapy.[142] The reasoning behind the greater protection for information disclosed

---

[139] *Id.* at 59,920.

[140] *See* Goldfarb, *supra* note 81, at ch. 4, 87 "Wouldn't sick people still use their doctors even if there was no assurance of confidentiality?".

[141] For instance, the rule permits the disclosure of health information when a health care official believes in good faith that the disclosure is "necessary for law enforcement authorities to identify or apprehend an individual . . . [b]ecause of a statement by an individual admitting participation in a violent crime that . . . may have caused serious physical harm to the victim." *See* Standards for Privacy of Individually Identifiable Information, *supra* note 135, at 59919. The needs of law enforcement trump patient confidentiality in this circumstance.

[142] Disclosure is not permitted to law enforcement when health care officials discover this information "[i]n the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure . . . or counseling or therapy; or . . . [t]hrough a request by the individual to initiate or to be referred for the treatment, counseling, or therapy . . ." *Id.*

in counseling is that revelation of this information would discourage people from seeking counseling that might enable them to avoid dangerous or harmful conduct.

H. Application to Contemporary Privacy Issues

A number of recent privacy policy initiatives and regulations incorporate contextual analysis. The Federal Trade recommends that for practices inconsistent with the context of their interaction with consumers, companies should give consumers choice, but that companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices.[143] The Obama Administration's consumer privacy report recommended a consumer privacy bill of rights containing a principle called "Respect for Context" and stating, "Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[144]

The new European General Data Protection Regulation calls for consideration of the "context in which personal data have been collected" in determining whether further use of information is compatible with the purpose for which the data were originally collected.[145] The Federal Communications Commission's proposal for broadband privacy, calls for opt-out consent for marketing communications-related services, but opt-in consent for other uses because they think that this approach is "consistent with consumer expectations" and observes the regulatory best practice that "consumer choice turns on the extent to which the practice is consistent with the context of the transaction."[146]

Nevertheless, how contextual analysis is supposed to be incorporated into privacy policymaker is far from clear. Helen Nissenbaum thinks that the current use of contextual analysis for privacy policymaking is a misunderstanding that reduces the sociological concept of social norm and social context to the notion of

---

[143] FED. TRADE COMM'N, *supra* note 3, at 36, 48.

[144] WHITE HOUSE, *supra* note 4, at 15.

[145] Council Directive 95/46/EC, art. 1(1), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en [https://perma.cc/4UEX-XR5V].

[146] Notice of Proposed Rulemaking, *supra* note 6.

a business environment or the use of a specific technology. In other words, it misses the social dimension of contextual analysis in favor of more familiar economic and technological assessments.[147]

Our discussion in the last section of how witness privileges preserve social norms of confidentiality allows us to formulate a series of policy-relevant steps that can guide the use of contextual analysis for privacy policymakers. A checklist would include the following elements:

- Identify the social context within which information is being used and what purposes the disclosure satisfies
- Assess how the information is used or is being considered for use in other contexts.
- Look for adverse consequences for data subjects or others resulting from this secondary use
- Examine the feedback mechanisms that might be activated, that is, look for ways in which people in the original context might withhold information as a way to protect themselves from these adverse consequences.
- Assess the extent to which these protective efforts will frustrate the purposes, goals and objectives of the original context.
- Compare the gains and losses across contexts

In the rest of this section, the notion of contextual harm is further defined and the notion is applied to the cases of genetic privacy, student privacy and online social networks.

I. Contextual Harm

We want to understand the way in which the lack of privacy norms can create a special kind of social harm that I call harm to a context. Consider the following passage from Posner:

> A in conversation with B disparages C. If C has a right to hear this conversation, A, in choosing the words he

[147] Nissenbaum, *supra* note 7, at 278.

> uses to B, will have to consider the possible reactions of C. Conversation will be more costly because of the external effects, and the increased costs will result in less, and less effective communication. After people adjust to this new world of public conversation, even the C's of the world will cease to derive much benefit in the way of greater information from conversational publicity, for people will be more guarded in their speech. The principal effect of publicity will be to make conversation more formal and communication less effective rather than to increase the knowledge of interested third parties.[148]

Posner immediately applies this line of reasoning to the student right of access to academic letters of recommendation under Family Education Rights and Privacy Act.[149] If a professor knows that a student is going to see his letter of recommendation, he will write it less candidly. If the recipient of the letter of recommendation knows that the student has not waived his right to see the letter, then he knows that the letter is less than candid, and discounts it. Students recognize this dynamic as well and so almost universally sign a waiver "because they know that the information value of a letter of recommendation to which the subject of the letter has access is much less than that of a private letter of recommendation."[150]

The feedback mechanism here is transparent and intuitive. People adjust their current behavior based on an assessment of what implications present conduct will have on their future prospects. Confidential letters of recommendation are more credible and effective than letters that they see. So the social situation stabilizes with confidentiality as the norm, even when a legal rule exists allowing it to be overridden.

Contextual harm occurs through this type of feedback mechanism. When people know that information from one context will be used against them in another context, they will refuse to divulge this information to begin with. This lack of privacy is injurious to the social practices that are constitutive of the original context.

---

[148] Posner, *supra* note 16, at 401.

[149] 20 U.S.C. § 1232g (1974).

[150] Posner, *supra* note 16, at 402.

It is important to isolate the elements of contextual harm and to do so it is helpful to imagine a status quo in which a social norm limits the flow of information from one context to another. This status quo is then disrupted by a changed social norm, or a legal override of the old norm. But that is not the end of the story. Participants recognize the new reality and restrict their information sharing. This new normal results in less contextual disclosure and a consequent inability of people to engage successfully or completely in the social practice. This is the harm to the social practice created by lack of a privacy rule.

Contextual harm results from a feedback mechanism that creates a new equilibrium after the shock of a disruptive change in privacy norms. The harm is measured by the difference in value between the new equilibrium that develops as a result of the change in privacy norms and the old equilibrium that obtained under the old privacy norm.

What powers the feedback mechanism that induces the change from one pattern of information exchange to a new one? The basic driving force of the feedback mechanism is that people will, if they can, withhold information when they think that information is likely to be used against them. But by withholding this information people are withdrawing from engagement in a desirable social practice or engaging in it in a less than complete fashion. The individuals suffer from doing this, but more importantly, there is a social cost, since the social practice falls into disfavor or disuse and the social welfare generated by the practice is lost.

To be clear harm to a context is not some irreducible harm that pertains to a thing called a "context." It does not arise willy-nilly independent of the wills, purposes and intentions of individual people. Instead, contextual harm takes place when rational people guided by their own self-interest take steps to protect themselves, if they can, from harmful uses of information. Ultimately, harm to a context means that people will not engage in the relevant social practice in ways that would be socially beneficial.

Contextual harm is not just harm to individuals. Clearly, there can be no social harm without individual harm. But some injuries are personal in the sense that the damage is restricted to the data subject. People can lose money; or find themselves inconvenienced or embarrassed or upset; they can lose jobs or insurance coverage or health care. Other damages are social in the sense that they adversely affect social relationships with people. Connections with lawyers, doctors and clergymen are social relationships; they exist only if people routinely play the social roles that are assigned to them within

these relationships. If they cease to exist as relationships, the loss is social, not simply individual.

Contextual harm is not quite the same thing as Nissenbaum's loss of contextual integrity. Nissenbaum *defines* contextual integrity as that which is preserved when informational norms are respected and that which is violated when informational norms are breached.[151] Contextual integrity just is the preservation of entrenched informational norms. Contextual harm, in contrast, is the decline in participation in a social practice because of a loss of contextual integrity.

The difference can be significant. Contextual integrity could be lost when a new informational norm replaces an old one, but because people still participate fully in the social practice under the new norms the context itself is not harmed.

Contextual harm can also be prospective. Some new uses of technology really do not present new social contexts. Online banking is still banking. Online shopping is still shopping. But sometimes a new socio-technical context arises because of the way technological possibilities are embodied in social practice. The arrangements of people, information flows, actors, and social roles are not simply technologically updated versions of old arrangements.

New social contexts do not have established norms that regulate information flows. So it is hard to define contextual harm in terms of violations of embedded informational norms that harm social practices. Still, information flows can harm a new or emerging social context. This can happen when the social benefits that the new technology makes possible cannot be realized or realized to their fullest in the presence of an adverse information flow.

J. Genetic Privacy

Legislation to restrict certain uses of genetic information outside the medical and research context provides a good example of how law can intervene to protect an informational norm under erosion by new technology and new business practices. As more companies began to use genetic information in a range of business decisions, the need to bolster the confidentiality of this information became urgent.

Genetic screening can detect susceptibility for certain disorders such as cancer, Alzheimer's disease and diabetes. This information

---

[151] Nissenbaum, *supra* note 7, at 140.

could be used to treat people and to conduct important research on the causes and treatment of genetically related diseases. It could also be used to deny insurance or employment to people based upon genetic dispositions to fall victim to expensive or disabling diseases.

The Genetic Information Nondiscrimination Act (GINA) addressed this use of genetic information outside the medical and research contexts. It prohibits U.S. health insurance companies and employers from discriminating on the basis of information derived from genetic tests.[152] Under this 2008 law, health insurance companies cannot reduce coverage or increase prices based on information about an applicant's genetic code. Employers cannot take adverse action against employees or potential employees based on genetic information. Nor can companies require that a person take a genetic test as a condition of obtaining health insurance or employment.

Why prevent this use of information? It is presumably accurate and predictive of both insurance risk and job performance. So a casual cost benefit analysis might say what's the harm? People who have genetic disorders should pay higher insurance and should not be eligible for certain jobs. Employers, insurers and individuals without genetic disorders will all benefit. On balance, society would be better off.

One response is that this is unfair, a violation of dignity and human rights of the individual. Another response is allowing genetic discrimination gets the cost-benefit balance wrong – in fact, people would suffer more from this than companies would gain. The contextualist approach allows us to see a rationale for the law that is independent of these human rights and utilitarian concerns. This rationale is that genetic discrimination would cause damage to medical and research practice.

If genetic information is generally available for business or other non-medical use, people will seek to protect themselves from these potential adverse effects of genetic testing and will do everything in their power to block the flow of this potentially harmful information. In particular, they will stay away from genetic testing. As the National Genome Research Institute put it:

---

[152] *See* Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008) (the law does not apply to the sale of life insurance, disability insurance and long-term care insurance).

> Many Americans fear that participating in research or undergoing genetic testing will lead to them being discriminated against based on their genetics. Such fears may dissuade patients from volunteering to participate in the research necessary for the development of new tests, therapies and cures, or refusing genomics-based clinical tests.[153]

This example brings out a contrast between the witness privilege cases and the use of genetic information. Court testimony that breaches confidentiality norms is usually public; the parties know that it takes place or that it is permitted under law. The harmful use of genetic information might be done in secret, without the data subject ever knowing about it. This brings up the question of disclosure requirements, which we address later in the Policy Considerations section.

In the case of genetic information, there was substantial public concern about the possible use of genetic information for insurance and employment eligibility. Some of the actual use might have been done in secret, but there was sufficient public acknowledgement of the practice so that people took into account the risk of this use when they considered whether or not to share genetic information for medical or research purposes.

GINA was designed to reassure people that it would be safe to reveal their genetic information. But the exceptions in the legislation work against this goal. The law does not apply to life, disability and long-term care insurance so that people who have a genetic predisposition to serious diseases might find themselves paying higher premiums or being denied coverage altogether for these insurance products. As a result, in 2014, 6 years after the passage of GINA, it is still the case that "many people are avoiding the tests" because of the possibility of these adverse consequences.[154]

---

[153], *Genetic Discrimination*, NAT'L GENOME RES. INST. (Jan. 21, 2017), https://www.genome.gov/10002077/ [https://perma.cc/8QJQ-2WY8].

[154] Kira Peikoff, *Fearing Punishment for Bad Genes*, N.Y. TIMES (Apr. 7, 2014), http://www.nytimes.com/2014/04/08/science/fearing-punishment-for-bad-genes.html?_r=0 [https://perma.cc/GUR5-7HZE] (patients are "concerned about the possibility of paying higher premiums or being denied coverage altogether because of the known existence of a dangerous mutation." Even those who are tested often ask "could we not put it in their medical record?" Doctors sometimes follow the American Medical Association code of ethics statement that "it may be necessary" for doctors to maintain a

This example illustrates some of the theme we saw in our examination of witness privileges: the basis for the privacy rules is the protection of an important social practice, the key question is the assessment of the risk to the social practice, and the notion that an uncertain confidentiality protection is often little better than no protection at all.

K. Student Privacy

Thinking of privacy as an aspect of social structure clarifies some aspects of the current debates about student privacy. In particular, the notion of contextual harm can illuminate the basis for the social norm and legal requirements that limit the use of student data to educational purposes.[155]

A widely shared and entrenched social norm is that information about students gathered as part of instructional activities should be used only for education. Students reveal information about their aptitudes, learning styles, learning performance and so on to their teachers in order to receive instruction. The educational records that preserve student – teacher interactions and assessments of learning should be used by teachers and school officials only for the purpose of fostering and improving student learning. It would be contrary to this informational norm for student information to be used for any other purpose, even a worthwhile one.

Current law and education codes and practices validate this norm. Regulations promulgated under existing federal law "do not permit PII (personally identifying information) from education records to be disclosed for purposes unrelated to education."[156] An industry-backed student privacy pledge commits providers of educational services to refrain from the use or disclosure of student information for targeted

separate file for genetic test results so the information is not sent to insurers. A small percentage of internists acknowledge that they hide or disguise genetic information).

[155] *See* Mark MacCarthy, *Student Privacy: Harm and Context*, 21 INT'L REV. OF INFO. ETHICS 13-24 (2014) (for a longer discussion of these issues).

[156] Family Educational Rights and Privacy, 76 Fed. Reg. 75,608 (Dec. 2, 2011) (codified at 34 C.F.R. § 99), https://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf [https://perma.cc/6T2R-F65A]. Further constraints on the use of student data without parental permission are imposed by the Children's Online Privacy Protection Act. *See* FED. TRADE COMM'N, THE COPPA RULE (2013) https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule [https://perma.cc/U8NB-HLBL].

advertisements to students.[157] The new student privacy law in California forbids companies that operate a site, service, or application that is used primarily for K–12 school purposes and that was designed and marketed for these purposes from using student information for targeted advertising.[158]

A draft Federal student privacy bill also addresses the targeted advertising issue. Under this bill, operators of student educational services cannot use student information to engage in or permit targeted advertising.[159] President Obama endorsed legislation incorporating this restriction of the use of student information to educational purposes. His Student Digital Privacy Act "would prevent companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school."[160]

Existing and proposed student privacy laws foster and protect the informational norms that grew up spontaneously within the educational context. What is the basis for the informational norm that restricts the use of student information to educational purposes?

Nissenbaum approaches this question through the lens of contextual integrity.[161] Her focus is on the need to retain the autonomy of educational practice, to insulate the educational process from other social practices and allow it to set and accomplish its own goals, values and purposes independent of the goals values and purposes of other social practices. The sharing of student information from the school with prospective employers might adversely affect the school context, causing teachers and students to give greater weight to practical considerations and reducing intellectual experimentation and training for democratic citizenship.

---

[157] STUDENT PRIVACY PLEDGE, (2017), http://studentprivacypledge.org/?page_id=45 [https://perma.cc/9AYU-AXY8] (the pledge was initially adopted in 2014 and now has well over 100 signatories).

[158] Cal. Bus. & Prof. Code §22584 (West 2016).

[159] *See* Student Digital Privacy and Parental Rights Act, H.R. 2092, 114th Cong. (2015).

[160] *FACT SHEET: Safeguarding American Consumers & Families*, WHITE HOUSE (Jan. 12, 2015) https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families [https://perma.cc/C2GF-72EC].

[161] Nissenbaum, *supra* note 7, at 169-171.

Sharing information outside the classroom for unrelated purposes can also generate self-protective behavior. Consider, for instance, the new technologies that can provide for personalized learning and the identification of students at risk.[162] Information generated through the analysis of detailed student information is useful to personalize learning and speed the mastery of diverse subject matters and it can also be useful to identify students at risk of failure so that they can receive special attention that will increase their chances of success.

But the same information can also be used to assess the eligibility of students for an array of offices and benefits. Is a student a good insurance risk? Is he likely to be an attractive consumer of specific products or services? Will he or she need government services? Will he be able to do this job? To the extent that this student information is predictive of competence in these other areas, there will be a push to use it for these purposes.

But using this kind student information for these non-educational purposes might undermine the trust that students and parents have in the integrity of the educational system. They will think that information made available to schools can now be used against them in jobs, insurance, credit and the availability of products and services. Many of them are likely to respond to this potential for harmful use of educational information by avoidance, hostility and withdrawal.

Since the use of educational technology and assessments can be required as a condition of attending school, it might be possible to block self-protective behavior through the use of mandates. But this ignores the real possibilities of resistance that would also undermine the educational context. An educational context of hostile, angry and withdrawn parents and students convinced that their school is working against their interests is not optimal.

These consideration, although powerful, do not end the discussion since the harm to the school context must be measured in some fashion against the gains to other contexts. It is not at all clear on what basis this comparison of gains and losses is to be accomplished. Nissenbaum recognizes the need to address this issue, but does not resolve it. For her, any balancing has to be done "against the backdrop" of educational values rather than "at large."[163] But when the values, purposes and ends of competing context are at stake it does no

---

[162] *See* MacCarthy, *supra* note 155, at 15-16.

[163] Nissenbaum, *supra* note 7, at 171.

good to conduct an inter-contextual evaluation in terms of the internal objectives of one of the contexts.

L. Online Social Networks

Nissenbaum's application of her contextual theory of privacy to online social networks is a good place to begin to understand how the notion of contextual harm clarifies the issues regarding privacy in online social networks.

She begins by thinking of the online world as an extension of the offline world. It is not a ". . . distinctive venue, sphere, place, or space defined by the technological infrastructures and protocols of the Net . . ."[164] Rather ". . . online activity is deeply integrated into social life in general and is radically heterogeneous in ways that reflect the heterogeneity of offline experience."[165] In particular, online social networking sites do not ". . . define a newly emergent, *sui generis* social context with its own internal rules." We cannot start from scratch and pretend that "there are no entrenched norms with which we need to contend."[166]

This leads to us to "look for the contours of familiar social activities and structures" so that "context-specific informational norms may be extended to corresponding online activities."[167] Specifically, online social networks are just extensions of the offline context of friendship.[168] So when online social network information is used in an employment context ". . . norms have been violated because recruiters and bosses have not respected transmission principles by scanning materials intended for friends . . ."[169] Similarly, the sale of social network profiles violates the traditional norms of friendship.[170]

---

[164] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS, THE J. OF THE AM. ACAD. OF ARTS & SCIENCES 32, 38 (2011).

[165] *Id.* at 37.

[166] Nissenbaum, *supra* note 7, at 223.

[167] *A Contextual Approach to Privacy Online*, *supra* note 164, at 39.

[168] Gordon Hull et al., *Contextual Gaps: Privacy Issues on Facebook*, 13 ETHICS & INFO. TECH. 33 (2011) (Nissenbaum's view of Facebook is similar to the view summarized by Hull et al., as "the cognitive model users bring to Facebook is offline friendship").

[169] Nissenbaum, *supra* note 7, at 225.

[170] *Id.*

Nissenbaum correctly asks, so what? Why should this violation of the traditional norms of friendship mean that these practices are "morally problematic?"[171] Why not adjust to the new practices?

Her unsatisfactory answer is that the new practices undermine the old contexts. How can one maintain a friendship, she seems to say, when the information one shares on Facebook can be passed on to an employer or sold to an information service provider?[172] But this is not enough. Offline information exchanges can continue unimpeded, but people will need to adjust their expectations for online exchanges. Once online social network information is regularly used in novel ways, people will become accustomed to it and expect it. Norms for social networks will evolve.

The notion of contextual harm can help here. As people become more familiar with how online social network information can be used against them, they will take steps to protect themselves. They will begin to assume that their Facebook information is part of their job application, their application for a loan or their attempt to get insurance. They will protect themselves by revealing only those aspects of their self that they think will pass the scrutiny of these eligibility tests.[173]

This self-protective behavior reveals a more fundamental reason for thinking of these out-of context information-sharing practices as problematic. They will lead to far less use and benefit from the new context of online social networks than is made possible by the design features of the technology itself. The magnitude of this harm to the social context itself needs to be assessed in designing privacy rules for online social networks.

The notion of contextual harm focuses our attention on the loss of these social benefits. The values, purposes, goals of social networks are still evolving, but these networks vastly expand the possibilities for expression and association. Online social networks allow for and encourage unprecedented new ways to engage with other people and to share thoughts, experiences, attitudes and beliefs. Sharing personal

---

[171] *Id.* at 227.

[172] *Id.* at 228.

[173] *See* Hull et al., *supra* note 168, at 5 ("Users could (and perhaps should) operate under the assumption that any information they put online is public and potentially available to anyone forever. Yet, this would clearly impact the social benefits of social network sites, as users would be forced to share less information than they would like, or simply accept all the privacy problems that result").

information on social media satisfies primal personal needs and desires and has substantial social benefits as well.

Disclosing social network information outside this context for eligibility decisions runs counter to these intrinsic expressive and associational purposes of online social networks. How much harm is done is an empirical question that should draw the attention of privacy regulators.

Considering what informational norms are needed to protect and promote the context of online social networks does not mandate any specific policy solutions. It directs attention to problems. One approach might be to follow the example of a proposed German law that would have prevented the use of Facebook information for employment decisions.[174] In contrast, the emerging policy approach in the United States is not to ban the use of social network information for out-of-context eligibility purposes, but to regulate its use for employment, insurance, and credit granting under the Fair Credit Reporting Act, which grants rights to data subjects and imposes responsibilities on those who use data for eligibility decisions.[175] This is one way to try to balance the usefulness of social network information for out-of-context purposes with the expressive needs of the context itself.

IV. POLICY CONSIDERATIONS

It is now time to draw together some of the implications of the previous discussions for policymakers. We start with stating clearly the principle of contextual harm, which has been implicit in our discussion up to now, and contrasting it with related principles.

---

[174] David Jolly, *Germany Plans Limits on Facebook Use in Hiring*, N.Y. TIMES (Aug. 25, 2010), http://www.nytimes.com/2010/08/26/business/global/26fbook.html [https://perma.cc/LF8E-Y35K] (the measure was never adopted).

[175] *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA,* FED. TRADE COMM'N (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed [https://perma.cc/FJS8-DBZH]. But notice that some social networks have chosen to ban the use of information about their users for eligibility decisions. See Facebook Platform Policy 3.15: "Don't use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan." *Facebook Platform Policy*, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/policy/ [https://perma.cc/HE95-P55U].

A. Principle of Prevention of Contextual Harm

We can abstract from the specific cases we have been considering a principle of prevention of contextual harm that can guide policymakers as they consider privacy laws or regulations:

> Principle of Prevention of Contextual Harm: A privacy rule restricting the flow of information out of a social context should be considered whenever such a flow causes or is likely to cause significant contextual harm.

As we have seen, such a principle is active in the witness privilege cases relating to lawyers, psychologists, religious counselors, and reporters, and the contexts that generate genetic information, medical information, social network exchanges, and student information. It provides a basis for saying that law should keep information within the social context where it was generated. It does not rely on individual rights to privacy or the avoidance of individual, personalized harm. The factual basis for this principle is that the out-of-context observability of information generated in a context alters contextual behavior itself. The normative basis is that when this altered contextual behavior is for the worse, defeating the intrinsic values, purposes and aims of the context itself, law might need to protect the social benefits that derive from a properly functioning social context.

The standard examples of contextual harm derive from an examination of established social practices, where stable traditional information norms have developed to ensure the confidentiality of communications within these practices. But contextual harm also extends to new socio-technical systems. Here expectations about information flows have not congealed into stable social norms and the analysis must be forward looking. The analysis must assess the potential advantages of new social practices inherent in the technical capabilities of new socio-technical systems and design informational norms that will foster these social practices.

One model for forward-looking privacy analysis is the role of privacy in the early days of the new United States republic. Privacy rules contributed to the expressive possibilities of a new national mail system that could link geographically disparate communities into the emerging political community that would be democratically governed

despite its territorial extent.[176] This new communication network, the national postal system, could function as an effective integrator of the new nation only if people felt comfortable sharing potentially sensitive information via mail. If they thought national censors or political opponents or business competitors would gain access to the information they put in letters, they would restrict their communications to what they thought safe for those audiences. In the late 1700s and early 1800s, there were no pre-existing social norms to rely on, because the technology was new, but the political benefits of a widely used national mail system could only be realized by imposing a legal rule of confidentiality.[177]

B. Respect for Context

A principle of respect for context has surfaced in recent privacy policy discussions in the United States. It is similar to, but not exactly the same, as the principle of prevention of contextual harm.

In its 2012 report on consumer privacy the Obama Administration embraced such a principle:

> Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.[178]

The key idea is that some data practices are "consistent with the context." The Administration's draft consumer privacy bill of rights introduced in 2015 replaced this idea with the notion of "reasonable in light of context." The draft bill requires companies to:

> . . . provide individuals with notice regarding personal data practices that are not reasonable in light of context at times and in a manner reasonably designed to enable individuals to decide whether to reduce their exposure to the associated privacy risk, as well as a mechanism

---

[176] *See* PAUL STARR, THE CREATION OF THE MEDIA 88, ch. 3-4 (2004).

[177] *See* Richards & Solove, *supra* note 2, at 140-45 (explaining the development of confidentiality in the mail system and its extension to the telegraph).

[178] WHITE HOUSE, *supra* note 4, at 15.

> for control that is reasonably designed to permit individuals to exercise choice to reduce such privacy risk.[179]

Some information practices are "reasonable in light of context" and some are not. The term "reasonable" serves to ensure that the test is not the empirical and possibly idiosyncratic reactions of specific people but the widespread expectations created by social norms of information flow. The further use of data collected in one context and used in another is not "reasonable in light of context" when it is not permitted by the informational norms that govern the original context.

The idea here is that when a use of information is expected in light of the context in which it was created, the need for legal privacy protections such as notice is reduced. However, legal privacy protections are needed when informational norms are breached.

The Federal Trade Commission's 2012 Report on Privacy also embodied this idea that consistency with context reduces the need for providing legal privacy protections such as choice:

> Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer . . .[180]

In its 2015 report on the Internet of Things, the FTC reiterates this contextual approach:

> . . . the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (i.e.,

---

[179] DEMOCRATIC MEDIA, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 9, https://www.democraticmedia.org/sites/default/files/field/public/2015/draft_consumer_privacy_bill_of_rights_act.pdf [https://perma.cc/T8WU-RNGR].

[180] FED. TRADE COMM'N, *supra* note 3, at 15.

> unexpected), companies should offer clear and conspicuous choices[181]

In this way, the principle of respect for context reduces to the idea of protecting reasonable expectations of information flow and use, where "reasonable" means "appropriate in the light of the informational norms of the context in which the information is collected."

The principle of respect for context embodied in these policy statements and draft laws is different from the principle of contextual harm. The principle of respect for context uses existing informational norms as touchstones for greater or lesser legal privacy protection. For example, the principle would allow information flows without notice and choice when the information flows are in accord with traditional expectations of the context in which the information is collected and used. But it would require that new, unexpected uses of information be subjected to a notice and choice regime and other privacy protections.

In contrast, the principle of contextual harm would look to evidence of withdrawal from the context or other behavior damaging to the goals, purposes and ends of a social practice as signs for the need for a legal restriction on information flow. Existing social norms would be prima facie guides to the likelihood of contextual harm, since the existence of a norm suggests it has a genuine social role, as in the examples we have considered throughout this paper.

But violations of expected social norms are only a prima facie guide to a problem. Existing informational norms might be outmoded or represent mere adherence to tradition without any contemporary social function. They might be "sentimental relics" like the adverse spousal testimony privilege.[182] In addition, opportunities provided by new socio-technical systems might justify unexpected information flows. Also, the affront to embedded social norms might not significant enough to undermine the context's ends, values and purposes.

---

[181] FED. TRADE COMM'N, INTERNET OF THINGS, PRIVACY AND SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/96BR-GSCQ].

[182] Hawkins v. United States, 358 U.S. 74, 81 (1958) (Stewart, J., concurring).

The following example shows how the FTC would apply its principle of respect for context in the case of a new Internet of Things application:

> . . . suppose a consumer buys a smart oven from ABC Vending, which is connected to an ABC Vending app that allows the consumer to remotely turn the oven on to the setting, "Bake at 400 degrees for one hour." If ABC Vending decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context of the consumer's relationship with the manufacturer, and the company should give the consumer a choice.[183]

In contrast, using the principle of contextual harm as a lens to analyze this example might result in a different way of thinking about it. A focus on contextual harm would lead us to ask whether this further use would be so upsetting to consumers that they would resist providing ABC Vending with any information associated with the smart oven. It would also lead us to ask whether there are any purposes, ends and goals of the new socio-technical system that would fail to emerge if people adopted a watchful or cautious attitude toward sharing information. Such a focus might also question whether the issue should be treated as an opportunity to discuss which norms are appropriate, rather than leave it to the one-on-one choice negotiations between a company and each individual consumer.

It is helpful to reformulate the Administration's principle that privacy practices should be reasonable in light of the context in terms of the notion of harm to a social context. This reformulation would state that secondary uses of information are unreasonable when they cause significant harm to the social context in which information was

---

[183] INTERNET OF THINGS, PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 181, at 40.

originally collected. This differs from the intended formulation in that it would make the touchstone the extent of actual harm to a social practice rather than whether the information use is consistent with entrenched expectations about use.

C. Purpose Specification

It is worthwhile to compare the principle of contextual harm with the familiar principle of purpose specification. According to this principle, personal data shall be "collected for specified, explicit and legitimate purposes should not be further processed in a way incompatible with those purposes."[184]

But what is "incompatible?" The Article 29 Committee, updating the EU's thinking on the issues of purpose limitation and secondary use in a 2013 Opinion, said further processing for a "*different* purpose does not necessarily mean that it is automatically *incompatible* . . . ."[185] Nor does the principle require that the further use be for a compatible purpose. The principle imagines that between compatible and incompatible purposes there might be purposes that are neither, that are neutral, not really related to the original purposes but also not

---

[184] General Data Protection Regulation, 2016 O.J. (L. 119) 35. Article 6(1)(d) of the 1995 Data Protection Directive contained a similar principle. *See* Directive 95/46/EC, 1995 O.J. (L. 281) 40. This principle is drawn from the 1981 Convention 108 for the Protection of Individuals with regard to automatic processing of personal data, which requires that when organizations engage in the "storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination" the personal data shall be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes." E.T.S. No. 108. The OECD Guidelines on the protection of privacy also contained a purpose specification principle: "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose." OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD pt. 2(9), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/FN2K-MRK9]. Article 8 of the Charter of Fundamental Rights of the European Union requires that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. *See* Charter of Fundamental Rights of the European Union, supra note 13, at 393.

[185] EUROPEAN COMM'N, ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 03/2013 ON PURPOSE LIMITATION 21 (2013), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [https://perma.cc/PP64-73SF].

clearly at variance from them. The principle allows further uses for these neutral purposes as well as for purposes that "fit closely with," that are clearly and obviously in harmony with, the original purposes.

The Article 29 Working Group says this "compatibility" test for further use includes in part an assessment of "the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use."[186] An incompatible use is for "an unrelated purpose that would not be reasonably expected by the data subject." An incompatible use is what "a reasonable data subject would assume . . . (is an) . . . entirely unrelated purpose . . . ." These concepts give a "strong indication" of use for an incompatible purpose. [187]

Compatibility can be restored by appropriate data protection measures even when the further use is for an unrelated purpose that a reasonable person would not expect in context. The Article 29 Working Group adopts a position similar to principle of respect for context used in recent U.S. privacy statements and draft laws, noting that where reasonable expectations are not met "additional safeguards, for example, informed consent of the data subjects, may help ensure that the further processing meets the expectations of the data subjects at the time of further use."[188]

The reliance on contextual analysis for assessing further use of information has moved from guidance by data protection regulators to a requirement of the new General Data Protection Regulation (GDPR). The GDPR retains the standard that the further use should not be incompatible with the purpose for which the data were initially collected.[189] But in making this determination the new data protection regulation says that data controllers must take into account context and consequences.[190]

What is the connection between the principle of contextual harm and the principle of purpose specification? The principle of purpose

---

[186] *Id.* at 40.

[187] *Id.* at 56-57.

[188] *Id.* at 13, 63 (considering online marketing, the Article 29 Working Party says: "tracking and profiling for marketing purposes can usually only be considered as compatible use if there is a lawful basis for the processing such as genuine, unambiguous, freely given and informed consent").

[189] General Data Protection Regulation, *supra* note 5.

[190] *Id.*

specification would apply more broadly than the principle of contextual harm, blocking uses for incompatible purposes rather than just for those that caused contextual harm. Data uses that involve contextual harm are uses for incompatible purposes, that is, they go beyond the original reasons for providing the information and touch on new uses in different contexts. But the converse is not true. Some incompatible uses might cause no contextual harm.

The principle of contextual harm might countenance further uses when embedded social norms have no contemporary social function, where opportunities provided by the new socio-technical system justify unexpected information flows, or where the affront to embedded social norms is not significant enough to motivate individuals to withdraw from the context in which they provided information or to otherwise alter their contextual behavior in ways that undermine the goals, purposes and values of the context. In these circumstances, the principle of purpose specification might provide for further privacy restrictions, while the principle of contextual harm might not.

GDPR calls for the consideration of whether the use of information for a further purpose is compatible with the original purpose for which the information had been collected. It might be helpful to incorporate the notion of contextual harm into this consideration. This could be done by interpreting Article 6(4)(b)'s reference to the "context in which the personal data have been collected" as calling for an assessment of the extent to which the purposes, goals and values of the context of collection have been harmed by the further use.[191]

D. Contextual Conflicts

We have seen several areas where information derived from one context is useful in a different context. The principle of contextual harm suggests that a privacy restriction should be considered when the additional use in a different context feeds back to work against the values, purposes and ends of the original context. But the needs of the different contexts are in conflict: what violates the integrity of one context might further the values, purposes and aims of a different

[191] *Id.* (calling for consideration of "the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller").

context. In these cases of contextual conflict, it does no good to draw on the internal purposes and values of each context. We need a principle or set of principles that can help adjudicate conflicts between contextual needs.

As we saw the case of witness privileges, genetic information, medical information, social networks and education, conflicts between contexts can be and are resolved. But it is hard to discern any principle at work other than intuitive case-by-case balancing.[192]

One consideration that can guide our thinking in this area derives from the self-defeating nature of some of the proposals for re-use of information out of its original context. The proposals are self-defeating because people react to the new regime of secondary, out-of-context use by restricting the flow of information into the new context. In the case of witness privileges for confidential communications, we saw that without the privilege the communication dries up and there is no additional information available to the court. The privileged information would never come into existence without the privilege.

In a similar way, any new proposal for out-of-context reuse of information might be self-defeating. Once people know about the new out-of-context reuse, and perceive it to be harmful or likely to be harmful to them, they react in a self-protective way to stop the communications that give rise to the harm. In the new equilibrium that results, there might be no new information for re-use because people do not disclose information anymore in the original context.

In these cases, the benefits to data users arise from surprising people with a new out-of-context information flow. But the costs fall on the data subjects. Once the data subjects realize that the new information use is harmful to them, they stop sharing for the original purpose and the secondary use dries up as well. In the new equilibrium, there is a net loss to society. Any advantage to the new context will be temporary and short-lived, while the damage to the old context will be permanent and irrevocable. To the extent that this result seems to be likely and significant, to that extent there is a case for not allowing information flow out of the original context.

---

[192] Nissenbaum, *supra* note 7, at 239 (recognizing the issue, but not resolving it. Nissenbaum states conflicts may surface "between or among contexts themselves . . . in collisions between library and law enforcement contexts, between health care and commercial contexts, and between health care and kinship contexts." Her proposed resolution is case-by-case: "I can think of no other way to deal with these except case-by-case, optimistic that some of these conflicts will be neutralized within the contexts themselves, a challenge for the future").

It is important to emphasize that this situation might call for norms backed by the law. The actors who might gain from the new use of information operate in one context; those who would lose operate in another. The gains to the winners do not matter to the losers; and the losses to those who suffer contextual harm do not matter to the winners. Marketers using student information to target ads to students could gain by even a temporary increase in the accuracy of their advertising, even if over time this would cause problems for education as schools, parents and students engage less and less with effective educational tools. The short-term gains fall on one party while the long-term losses affect others.

The losses from contextual harm are also likely to be irreversible. Once people lose trust in the limitations of information use to the original context, it is difficult to persuade them to part with information going forward. The downside risks of harm to valuable social practices cannot be ignored or downplayed. We need to be sensitive, as Post suggested, to the "extreme fragility of privacy norms in modern life."[193]

Our examination of witness privileges revealed the dangers of leaving the resolution of contextual conflicts to a case-by-case balancing. If the privilege exists only as an individualized, after-the-fact, and fact-based case-by-case determination, it might not be effective.[194] An uncertain privilege is "little better than no privilege at all."[195]

A limitation on out-of-context use has to be adopted as a rule, not as a consideration to be taken into account on a case-by-case basis. If there are to be exceptions from such a limitation, as there might need to be to avoid the rigidities of absolutism, they should be clear and limited, with a view toward creating accurate expectations in the minds of the relationship participants. People should not need to consult lawyers to understand whether their information is protected in a certain context.

---

[193] Post, *supra* note 58, at 1010.

[194] Jaffee v. Redmond, 518 U.S. 1, 17 (1996) (noting "[m]aking the promise of confidentiality contingent upon a trial judge's later evaluation of the relative importance of the patient's interest in privacy and the evidentiary need for disclosure would eviscerate the effectiveness of the privilege").

[195] Upjohn Co. v. U.S., 449 U. S. 383, 393 (1981).

The lack of guiding principles in assessing cross-context data use will be increasingly problematic in the age of big data analytics. Big data analytics is a natural evolution of older data analytics methodologies. It involves new processing techniques for analyzing data of increased variety, velocity and volume. Big data sets often consist of unstructured data such as text, images or video, or semi-structured data such as web logs. As a result, they require analytical techniques different from those typically used to analyze structured databases.

Data for analytical purposes will increasingly come from several sources including traditional enterprise data, machine generated data, sensor data and social media data. Big data works best when it can combine, merge or link data from multiple sources and different contexts to see what new insights can be derived by looking at the data as a single picture of a complex social reality.

But this is precisely where we need to be careful. In the age of big data analytics, machine learning and artificial intelligence, data increases in value in part because it has been separated from the original purpose of its collection.[196]

It is important to emphasize that the data in this new big data world is decontextualized. The contextual source of the information is less important than whether it contributes to accurate predictions. Rather than create incentives for organizations to be sensitive to the context from which information is drawn, the merging and linking of data from a vast array of different contexts encourages the idea that the resulting portrait is independent of any social context. It is a contextless collection of information about a person that does not derive its validity or meaning from any specific social context and is available for use in any and all specific contexts.

In this circumstance, there are few incentives to examine the feedback effects on the contexts from which the information is drawn to see if self-protective behavior undermines these contexts. For this

---

[196] *See generally* VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013). "With big data, the sum is more valuable than its parts, and when we recombine the sums of multiple datasets together, that sum too is worth more than its individual ingredients." *Id.* at 108. "The extra cost of collecting multiple streams or many more data points in each stream is often low. So, it makes sense to gather as much data as possible, as well as to make it extensible by considering potential secondary uses at the outset." *Id.* at 109. "[. . .] [D]ata intermediaries will emerge that are able to collect data from multiple sources, aggregate it, and do innovative things with it." *Id.* at 135. "[. . .] [D]ata is now raw material entering the marketplace; an asset independent of what it had previously aimed to measure." *Id.* at 136.

reason, there is a need for a special effort to focus the attention of analysts, scholars, policymakers, and business executives on the possibilities of contextual harm from these feedback mechanisms.

E. Completeness

We have been exploring the way in which privacy rules operate to allow people to engage in important social activities. In the absence of these rules, people might take self-protective actions that would impede context-appropriate conduct, to the detriment of the larger society that relies on the functioning of these social practices.

But what about areas where self-protective actions are difficult or impossible to take? Or circumstances where people do not know the extent to which information is shared out-of-context? Here people do not have the knowledge, capacity or ability to withdraw from the social activities, and so they continue to engage in context-appropriate behavior, regardless of the harmful consequences they will suffer as a result. There might be adverse consequences for individuals in continuing to participate in the social activities in question with no real capacity to withdraw.

Policymakers might want to protect people from these adverse consequences, but cannot justify it on the basis of contextual harm, since, without self-protective actions, there is no harm to the context. What should be done when there seems to be a problem but the principle of prevention of harm to contexts is silent?

The question raised is really whether the principle of contextual harm is meant to be complete, to provide a rationale for all privacy rules so that if a privacy rule does not protect against contextual harm its basis is suspect.

The answer is that the principle of preventing contextual harm is not meant to explain or justify all privacy rules; not all privacy problems are based on contextual harm. When withdrawal from a social practice is difficult or impossible, and yet imposes substantial harms on individuals who continue in the practice, then a rationale for protective measures could still be constructed and could be *related to* contextual matters. Policymakers can often reason that the continued functioning of the social practice is socially desirable and law should not permit the imposition of unfair penalties on people for engaging in these socially worthwhile activities. But in these cases, the basis for the restriction cannot be harm to the context, but rather whatever makes the penalty unfair. If people continue to engage in the context, and yet the flow of information out of the context imposes harms that

we think need to be avoided through a restriction on the information flow, then the basis for the restriction cannot be harm to the originating context. It must be an independent normative rationale. Any such independent rationales can be drawn from the traditional human rights and utilitarian frameworks.

Contextual harm might seem to be a thin basis for privacy rules, since one way to prevent contextual harm is to keep secret any out-of-context harmful use of information. Without knowledge, there is no feedback mechanism and without the feedback mechanism there is no contextual harm.

Secret out-of-context use of information against the interests of the data subject seems to be almost a paradigm case of a privacy invasion. A disclosure requirement or a notice and consent requirement might remedy this privacy invasion, but there is no basis in the notion of contextual harm to require it.

This concern is not a practical one. It is usually not possible to keep harmful further use of information secret, at least when the further use is widespread and legal. As we saw in the case of genetic information, even the fact that the information could be used against people is often enough to prompt the feedback mechanisms that would enable people to take protective action that damages the context in which the information was collected.

V. CONCLUSION

Thinking of privacy as an element of social structure is a fruitful way to approach privacy policy. It extends the range of considerations that should be brought to bear when a new information practice arises. In addition to concerns about human rights and aggregate individual harm, it directs attention to the possibility that valuable social practices will be damaged from information flows.

Our review of several versions of the idea that privacy is an element of social structure revealed a rich mode of analysis that has yet to be fully utilized. The discussion of the rationales for various witness protections make it clear that seeking to prevent contextual harm has been a familiar tactic in the justification of legal rules protecting the confidentiality of various relationships. Examining genetic privacy, online social network privacy and student privacy through the lens of contextual harm revealed aspects of these problems that might otherwise have been hard to detect.

For the future, I recommend the incorporation of assessments of contextual harm into policy making. To that end, I compared a

principle of contextual harm with familiar principles of respect for context and purpose specification, showing what they had in common and where they differed. A crucial task, especially in light intrinsic drive of big data analytics to decontextualize data, is to examine principles that might enable us to make better assessments of cross-context data use.